0981 KABA ELECTRONIC SECURITY

Branded worksection

This branded worksection *Template* has been developed by NATSPEC in conjunction with **Kaba Australia Pty Ltd** and may be used whilst the Product Partner is licensed to distribute it. The copyright remains with NATSPEC. As with all NATSPEC worksections, it is the responsibility of the user to make sure it is completed appropriately for the project. The user should also review its applicability for local conditions and regulations. Check www.natspec.com.au for the latest updated version.

Worksection application

This branded worksection *Template* is applicable to the provision of **KABA** access control and security alarm systems in buildings. It relies generally on AS 2201, and includes local alarm systems, centrally monitored systems, access control systems and closed circuit television.

This worksection is intended to supplement the standard and to cover general commercial grade systems, of the sort likely to be installed in office buildings, residential apartments, nursing homes and similar buildings. This worksection can also be used for institutional projects such as schools and technical colleges by the inclusion of appropriate details in the project specification.

See NATSPEC TECHreport Selection and design of Building IT systems for an overview of IT systems required for buildings, how different IT system components are provided and the interrelationship of the relevant NATSPEC worksections.

***Guidance* text**

All text within these boxes is provided as guidance for developing this worksection and should not form part of the final specification. This *Guidance* text may be hidden or deleted from the document using the NATSPEC Toolbar or the hidden text *Hide* and *Delete* functions of your word processing system. For additional information visit FAQs at www.natspec.com.au.

***Optional* text**

Text in this font (blue with a grey background) covers items specified less frequently. It is provided for incorporation into *Open* text where it is applicable to a project.

Related material located elsewhere in NATSPEC

If a listed worksection is not part of your subscription package and you wish to purchase it, contact NATSPEC.

Related material may be found in other worksections. See for example:

- *Building IT components*.
- *KABA door hardware*.
- *Building management systems*.

Cross references

Worksections that cross reference this worksection are:

- None.

Material not included in NATSPEC

Some projects may include items not covered by NATSPEC. For these you may need to create new text, or modify this text or a suitable worksection. For example:

- There are many different types of intruder alarm systems and associated equipment currently available which comply with the relevant Australian standards. While each of these systems may be intended to perform the same task, they each generally have their own unique operating systems and protocol. The electronic security industry is also subject to continuing product improvement and rapid development.

Documenting this and related work

In addition to the schedules in the specification you may document the work as follows:

- Provide a block diagram or single line diagram on the drawings.
- Provide plan layouts showing the location and layout of all equipment and cable routes.
- Coordinate vehicle access control equipment with the architecture.

Specifying ESD

Refer to the NATSPEC TECHreport - *Specifying ESD*. The following may be specified in the worksection:

- Materials and products selection options.

1 GENERAL

1.1 RESPONSIBILITIES

Kaba Australia Pty Limited is a member of the worldwide Kaba Group. KABA has become an important security leader in Australia providing access control systems and secure door hardware to a range of industries. The Kaba Group has incorporated renowned companies such as Ilco, Unican, Silca, Gard, Mas Hamilton, Gege and Boyd.

The company delivers exceptional products to the market including key and cylinder systems, electronic access systems, pushbutton locks, safe locks, door hardware and locksmith products. Kaba also provides automatic door systems, hotel lodging, physical access systems and workforce management solutions.

General

Requirement: Provide KABA electronic security systems as documented and as follows:

- Remote monitoring system.

Documented is defined in the *General requirements* worksection as meaning contained in the contract documents.

A local security monitoring system will generally only be required if the building has the appropriate personnel to manage and react to the security system data. If required schedule its functions in detail. Use the *Building IT components* worksection as necessary.

- Access control management system.
- Intruder detection system.

Available on demand.

- Video monitoring.

Available on demand.

- Intercom system.

Available on demand.

Security classification: As documented in the **System description schedule**.

System communications: As documented in the **System description schedule**.

System provider

Electronic security system provider: A licensed security organisation only.

Depending on the state or territory this means licensed by the relevant statutory authorities or industry association.

Surge protection devices (SPD)

General: Provide all mode metal oxide varistor based series connected SPD to protect final equipment in racks and cabinets.

Standard: To AS 4262.1 and AS 4262.2.

Surge Rating: $I_{max} \geq 20$ kA per phase.

Residual Voltage: $U_p < 600$ V.

Visual indicator: Provide visual indication of SPD status.

Enclosure and installation: House SPD in a metal enclosure and protect with a suitable rated circuit breaker equal to or less than the load current rating of the SPD.

1.2 COMPANY CONTACTS

KABA technical contacts

Website: www.kaba.com.au.

1.3 CROSS REFERENCES

General

Requirement: Conform to the following worksection(s):

- *General requirements*.

The *General requirements* worksection contains umbrella requirements for all building and services worksections.

- *Cable support and duct systems*.
- *Uninterruptible power supply*.
- *Telecommunications cabling*.

List the worksections cross referenced by this worksection. The *General requirements* worksection references the *Common requirements* subgroup of worksections. It is not necessary to repeat them here. However, you may also wish to direct the contractor to other worksections where there may be work that is closely associated with this work.

NATSPEC uses generic worksection titles, whether or not there are branded equivalents. If you use a branded worksection, change the cross reference here.

Coordinate the following with other worksections of the specification:

- Location of power outlets for electric door strikes or locks if required.
- Locations of concealed conduits to door frames for reed switches and electric door strikes or locks.
- Type and dimensions of electric door strikes or locks to enable door frames to be prepared off site.
- Location and type of intercom system if applicable.
- Location and type of closed circuit television system together with auxiliary equipment or accessories.
- Use of telecommunications cabling. See, for example AS/NZS 2201.5 clause 2.1.

1.4 SYSTEMS

Access management system

Requirement: Provide an access management system capable of protecting buildings, rooms and areas, and performing monitoring and control functions.

The access management system performs security-related and specific organisational tasks cost-effectively while taking account of system integration and data management requirements.

Basic elements: Provide the following:

- Central management system with client/server and/or Web Client architecture.
- Recognition of identification devices/identification of authorisation (e.g. reader with contact-free reading system, RFID, individual identification using biometric technology).
- Physical barrier (e.g. door, gate, space, isolation, barrier, structural design).
- Logical barrier: PC authorisation reader.
- Sensor technology to record real passage situation.
- Locking technology as connecting element between identification and granting of access.
- Central authorisation management for wired and non-wired access points (on-line and stand-alone components).
- Integrated time and attendance (T&A) functions.
- Locking plan management.
- Parking management.
- Visitor management.
- Tenant management.
- Contractor management.
- Elevator control and depot management.
- Alarm management with interactive graphic control.
- Badge management: Creation, programming and management.
- Interfaces to the following:
  - . Intruder detection system (IDS).
  - . Fire detection system (FDS).
  - . Video surveillance (CCTV).
  - . Building services management (BSM), integrated building management systems (IBMS) with ODBC and OPC).
  - . Human resources (HR) systems.
  - . T&A systems, payroll accounting (XML).
  - . IT infrastructure (LDAP, SSO).

Solution concept: A modern, open, flexibly extendible system architecture, with the following features:

- Modular in structure.

- Providing coordination of the various areas of activity and taking account of the process-based interaction at different security levels (means of identification, the combination of mechanical, mechatronic locking system and electronic access control).
- Capable of integration into existing IT infrastructures.
- Open and accessible to original equipment manufacturer vendors at any time.
- Offering long-term compatibility of the system elements.
- Vendor: Long-standing experience and a sound financial background.

1.5 STANDARDS

If specifically required for the project, require authorisation of equipment by the Security Construction and Equipment Committee (SCEC). The SCEC is a standing interdepartmental committee responsible for the evaluation and endorsement of security equipment for use by Australian Government departments and agencies.

Intruder alarm systems

AS 2201 covers intruder alarm systems; it does not cover access control or closed circuit television systems. The standard provides detailed coverage of the design, installation and operation of alarm systems, including the performance requirements of detection devices, monitoring stations, wire free systems and alarm transmission.

General: To AS/NZS 2201.1.

AS/NZS 2201.1 covers general design, construction, installation and maintenance of intruder alarm systems, as well as outlining, in Section 5, the minimum requirements for any maintenance agreement.

Alarm transmission system: To AS/NZS 2201.5.

AS/NZS 2201.5 includes alarm transmission via dedicated paths, switched networks and wire free systems.

Internal detection devices: To AS 2201.3.

AS 2201.3 nominates the minimum performance and reliability standards including false alarm rates for security alarm detectors.

Wire free systems: To AS 2201.4.

AS 2201.4 covers the classification, construction and installation of systems where component parts are linked by RF or ultrasonic signals.

CCTV systems

General: To AS 4806.2.

Remote monitored systems: To AS 4806.4.

AS 4806.2 covers both design and installation issues. Some of these design issues will be incorporated in the documents. Care must be taken that this reference to AS 4806.2 does not override the other documentation.

1.6 MANUFACTURER'S DOCUMENTS

Technical manuals

General: Technical manuals are available on request.

Website: www.kaba.com.au.

1.7 INTERPRETATION

Abbreviations

General: For the purposes of this worksection the following abbreviations apply:

- BSM: Building services management.
- CCTV: Closed circuit television.
- ERP: Enterprise resource planning.
- FDS: Fire detection system.
- HCM: Human capital management.
- HR: Human resources.
- IBMS: Integrated building management systems.
- IDS: Intruder detection system.
- IT: Information technology.
- LAN: Local area network.
- LCD: Liquid crystal display.

- LDAP: Lightweight directory access protocol.
- LED: Light emitting diode.
- ODBC: Open database connectivity.
- OPC: Object linking and embedding for process control.
- PC: Personal computer.
- PIN: Personal identification number.
- RAID: Redundant array of inexpensive/independent disks.
- RFID: Radio frequency identification.
- SAP HR: Systems, applications and products in data processing human resources.
- SME: Small medium enterprises.
- SPD: Surge protection device.
- SQL: Structured query language.
- SSO: Single sign on.
- T&A: Time and attendance.
- WAN: Wide area network.
- XML: Extensible markup language.

Edit the **Abbreviations** subclause to suit the project or delete if not required. List alphabetically.

Definitions

General: For the purposes of this worksection the following definitions apply:

- Web client: Provides common methods for sending data to and receiving data from a resource identified by a URL.
- Power chute: A computer program to control uninterruptible power supplies.
- Metal oxide varistors: Semiconductors that protect electronic components and systems from transient voltage.
- Mechatronics: The synergistic integration of mechanics, electronics, control theory and computer science within product design and manufacturing in order to improve and/or optimise its functionality. (French standard NF E 01-010).

Edit the **Definitions** subclause to suit the project or delete if not required. List alphabetically.

1.8 SUBMISSIONS

Records

General: Submit records to AS/NZS 2201.1.

Licence: Submit copy.

Samples

Specify the samples required, particularly where there are architectural or building considerations to be taken into account.

General: Submit samples of the following:

- Door contacts and reed switches.
- Detection devices.
- Activation devices.
- Key or card readers.
- Electric door strikes and door release devices.
- Duress alarm switches.

Shop drawings

General: Before commencing work, submit shop drawings to a scale that best describes the detail, showing the following:

- Schematic diagram of all systems.
- Panel layouts and dimensions.
- Power supply requirements.
- Wiring access necessary for door frames.
- Cut out dimensions.

- Fixing provisions for cameras and monitors.

Include the following information in the contract documents, as applicable, so that the contractor can prepare the shop drawings:

- Details of existing system if interconnection is required.
- Location of main alarm panel and sub panels.
- Location of controlled and monitored doors.
- Lift car readers.
- Monitoring if remote, and the location of the security monitoring base, and location and type of alarm registration.
- Rooms or areas to be covered by internal motion detectors.
- Location and description of CCTV cameras and monitors.
- Location and capacity of intercom stations.

Technical data

See AS/NZS 2201.5 clause 3.3 for example.

General: Submit data showing dimensions and space requirements for the following:

- Door contacts and reed switches.
- Detection devices.
- Activation devices.
- Electric door strikes and door release devices.
- Television monitors, cameras and associated equipment.
- Intercom stations.
- Vehicle control systems.
- Duress alarm switches.

2 PRODUCTS

2.1 GENERAL

Product substitution

Other electronic security systems: Conform to **SUBMISSIONS, Substitutions** in the *General requirements* worksection.

The *General requirements* worksection clause sets out the submissions required if the contractor proposes alternative products. Refer also to NATSPEC TECHnote GEN 006 for more information on proprietary specification.

Alarm system panels or processors

Capacity: Provide separate sectors for each nominated internal zone, and for normally-closed and normally-open perimeter zones.

Specify the number of sectors required, generally separating internal zones from perimeter zones.

Sector time delay: Provide adjustable time delay entry/exit for each sector, with adjustment range 0 to 30 s.

Identify the areas requiring delayed entry sectors – these should be kept to a minimum – and indicate the time range required. This should just be sufficient for a person familiar with the system to activate it.

Batteries and chargers: Provide a sealed battery and charger system contained within each control panel with capacity as documented.

Delete if not required. Include the functional operating time in the **System requirements schedule** to enable battery size to be determined. It is expected that, generally, sealed batteries will be used in each panel.

Uninterruptible power supply

General: Provide a dedicated uninterruptible power supply and connect to the security systems.

Include or refer to *Uninterruptible power supply* worksection as necessary.

Retain if required, to prevent loss of system memory. On larger installations, the security control room sometimes requires a UPS to provide power to the security panel, as well as to the CCTV system. Specify this if it is not to be provided by others.

Capacity: At least 15 minutes, for the complete system in normal operation.

Activation

Activation devices: Provide keypads, cards, card readers and other activation devices for access control and intruder alarm systems as documented.

External: Provide weatherproof (IP56) hoods or housings for external units.

Default mounting height: 1100 mm above floor level.

External audible and visual alarms

General: Provide corrosion-resistant weatherproof metal enclosures containing sirens and blue strobe lights. Fix in locations not readily accessible without a ladder.

In some cases local sounding bells or sirens are not required where remote monitoring is provided. Consider telephone dialler.

Anti-tamper devices

These generally take the form of micro-switches or similar devices in alarm panels or exposed equipment.

Anti tamper devices: Provide anti-tamper devices to control panels, external equipment, control and activating devices, and access control devices.

Function: To register an instantaneous alarm if covers are removed or vital wiring is disconnected.

Alarm circuit supervision

To register an alarm when wiring to devices is cut or short circuited. This can often consist of an end-of-line resistor or module connected via wiring within the cable to the detection devices.

Alarm circuit supervision: At each detection device, provide alarm circuit supervision by means of an end-of-line device connected via a separate circuit within the cable.

Function: To register an instantaneous alarm if cable characteristics change, such as when cut or short circuited.

Event logging

Printer: Provide for event logging from the alarm and access control panel at a local security monitoring system.

Amend to suit project requirements. Generally event logging will not be required unless a local monitoring system is being provided.

Function: To generate a report showing, as a minimum, the date, time and category of alarm initiations and access control entries.

Remote monitoring

Delete if monitoring is not required.

Consider interfacing with an existing security or building management system. Subject to spare capacity, alarm outputs for monitoring purposes can generally be connected without difficulty. However, higher levels such as remote setting and monitoring of computer based systems may restrict the selection of the new system.

Ascertain method of connection to remote base station, if required. Allow for the work associated with connection, such as charges for line rental and connection.

Duration: Provide remote monitoring for the duration of the defects liability period.

Contractor to select method.

For local monitoring, indicate the location of the monitoring system or security control room, and whether additional mimic panels are required. For connection to central stations see AS/NZS 2201.5.

For remote monitoring, specify the method of connection and the location of the monitoring station or base. This will usually be via the telephone network or, in some cases, a leased line. Less complex systems are usually connected via the telephone network to a location from where a key holder or other responsible person can respond. Indicate the level of control required from a remote location, such as resetting alarms, and securing the system.

Monitoring system: Provide a monitoring system in the alarm panel or processor for transmission of alarms and monitoring of the system by parties responsible for attending to alarms.

2.2 ACCESS MANAGEMENT SYSTEM

System architecture

System functions: Provide an access or workforce management solution in conformance with the following:

- Multi-level security: Maintain full operation and security even if communication with a higher level is interrupted.

- Existing networks: Employ existing networks (LAN/WAN) and web service infrastructures/IT environments and standard components that can operate with existing security mechanisms such as firewalls or data encryption.
- Freely scalable: Provide system components which are scalable without limitation and able to connect to external systems.

Prepare a block diagram.

Interactive worksection/Web Client (data entry, operation, monitoring): Include the following functionalities:

- Data entry, monitoring and system operations using a standard PC with a Windows operating system (e.g. XP/Vista).
- Compatibility with PCs in the existing work environment.
- Option to connect to a USB desktop reader for rapid data entry and additional functions such as the programming/validation of badges.
- Utilisation of Web Clients using standard web browsers (e.g. Microsoft Internet Explorer or Firefox).
- Utilisation of Web Clients without the need for installation of additional software programs.

Database server: Include the following functionalities:

- Central server for the management of all data (central database).
- Support for Oracle and Microsoft SQL Server databases.
- Independence of the operating system (e.g. Windows Server, Unix).
- Central maintenance and serviced by the IT department (e.g. data backup, data recovery, availability/reliability).
- Data import/export from predecessor/external systems using standard database tools.
- Data access security.
- Distribution of the relevant data to the communication hubs.

Web server: Include the following functionalities:

- For the use of Web Clients, the distribution of data to the corresponding workstations.
- For an SME access management system, physical installation of the web server on the database server.
- Central maintenance and service by the IT department (e.g. data backup, data recovery, availability/reliability).

Communication hub: Include the following functionalities:

- Control of data traffic between the local networks (sub-networks) and the database server, including in the event of an interruption to communication or a network fault.
- Option for additional communication hubs, e.g. an independent subsystem for each additional building or branch office.
- Connectivity to SAP, building services management systems and external systems using standard interfaces such as OPC, XML Syntax, LDAP.

Access hub: Include the following functionalities:

- Control and monitoring of doors and other building installations independently.
- Control up to 64 access points per access hub.
- Level of security maintained even if there is no connection to the communication hub.

Door manager (door controller): Include the following functions:

- Installation within secure indoor area.
- Independent control and monitoring of one door with up to two registration units/readers or two doors, each with one registration unit, including all door components.
- Fully operation and maintenance of the security level, even if there is no connection to the communication hub.
- Control of up to 32 door managers per access hub.
- Direct connection to extension modules (inputs and outputs) for elevator control or controlling depot boxes without additional wiring.

Ethernet access manager: Include the following functions:

- Option for direct connection to a network (LAN/WAN) in the secure indoor area.
- Independent control and monitoring of one door with up to two registration units/readers or two doors, each with one registration unit, including all door components.
- Secure linking of external branch offices to company headquarters with a VPN connection.
- Maintenance of full operation and security level of the door managers even if there is no connection to the application.
- Direct connection to extension modules (inputs and outputs) without additional wiring.

Basic system

The basic system has an open architecture, supports Oracle and Microsoft SQL Server databases, covers current interface standards and supports the basic functions listed below.

Selections: Kaba exos 9300 Basic System.

Type: Administration station software licence for 1 operator.

Optional: Kaba exos 9300 SBS Limited Basic System for up to 500 persons for access control and T&A.

Requirement: Include the following functionalities:

- Freely scalable system solution with full upwards compatibility allowing implementation of organisational and technical security requirements in a flexible, modular manner.
- Open system architecture: Uses existing IT infrastructures and IT environments.
- Support for Oracle and Microsoft SQL Server databases.
- Distributed intelligence with a decentralized architecture to ensure maximum operational reliability and stability.
- Management, alarm and logging functions.
- Support of Single Sign On (SSO).
- Staff data management: Include the following:
- Registration and management of staff data, including photo.
- Assignment of access rights and T&A models.
- Generation and detailed evaluation of reports and statistics based on defined criteria.
- System management: Include the following:
- Central configuration and management of peripheral devices in the system.
- Same system management for both on-line and stand-alone components, that is non-wired access points.
- Management of mechanical locking systems of 50 components.
- Logging: Recording of all events including alarms, instances of access, system errors, security-related user actions, at all times in both on-line and off-line mode.
- Monitoring and control of various alarm zones in connection with an intruder detection system.
- Option to transfer the access rights (including CardLink™) and T&A data from an active badge to a transition badge if required.
- Remote maintenance option: Connection between headquarters and a remote branch office over a phone line.

Performance features

Number of persons: Unlimited.

Number of badges: Unlimited.

Number of access points (doors): Unlimited.

Number of communication hubs: Unlimited.

Staff data management:

- Detailed personal data (including photo).
- 5 freely definable checkboxes.
- 5 freely definable data fields (e.g. security check carried out).
- 10 free text fields (e.g. vehicle data).

Management of the following:

- Administration areas.

- Users and user groups with individual rights.
- Company hierarchies (mapping of organisational structure).
- Individual, regional exceptional days (public holidays) - System parameters (display of current operating states).
- Control profiles (time control of access points).

Blacklist function.

Event and alarm processing (storing of checklists, definition of actions).

Automatic program starts (programs, script files, operating system commands).

Logbooks in real-time display: System logbook, alarm logbook, error logbook, access logbook, T&A logbook, display logbook, download logbook, audit logbook, depot logbook, parking logbook, visitor logbook, badge logbook.

Change between summer time/daylight saving time: Automatic changeover.

Logbook size: Unlimited.

Unicode, that is, freely selectable dialog language.

Remote Maintenance Equipment/Remote Connection of Branch Offices

Selections: Kaba exos 9300 Basic System.

The customer/user/system operator is to provide a freely accessible phone connection.

Requirement: Include the following functions:

- Connection between remote access hubs or terminals and communication hubs via phone line (ISDN or analogue) using an ISDN or analogue modem (call service).
- Remote user support and troubleshooting.
- Option for remote maintenance, periodic checks and program modifications/adaptations through the central access management system.
- Option to establish or clear a connection with the central management system automatically, manually or by time-controlled means.
- Connection with TCP/IP routers and automatic clearance by the access hub (call-back function) if an alarm is triggered in the branch office (substation).
- Access to several modems for each management system.

Dialogs/Web clients

Dialogs/Web clients allow several people to operate the system operation, record data, evaluate and monitor alarms simultaneously. The Dialogs/Web Clients offer the following functions as an optional module in the integrated access management system.

Selections: Kaba exos 9300 Basic System.

Type: Administration station software licence for 1 operator.

Number of operators: Licences available for 1, 3, 6, 10, 30, 60 operators. Edit as required.

Option 1

Type: Web Client software license for x supervisors (1, 3, 6, 10, 30, 60, 100, 300).

- Access to the access management system from any workstation.
- Supervisor able to view and edit the data of assigned employees.
- This licence includes all functions of the SW licence Web Client ESS for employees licence so that a supervisor does not require an additional licence to view or edit his personal data.

Option 2

Type: Web Client software license for x supervisors (1, 3, 6, 10, 30, 60, 100, 300) plus T&A functions software license for supervisors.

- Time data sheet display and corrections of assigned employees.
- Signature function for employees and supervisors.
- Planning board display, i.e. graphic representation of approved half-day or whole-day absences in the past and into the future, work profiles and error codes (i.e. in the event of violation of core time).
- Integrated workflow for the approval of holidays and other periods of absence.

Option 3

Type: Web Client ESS software license for x employees (100, 300, 600, 1000, 3000, 6000, 10 000).

- Access to personal logbook.
- Update to personal CardLink authorisations.

- PIN code change to registration unit with PIN code keypad.

Option 4

Type: Web Client ESS software license for x employees (100, 300, 600, 1000, 3000, 6000, 10 000) plus T&A functions for employees software license.

- Display time data sheet.
- List of absentees showing reason for absence.
- Record coming/going (with reasons) if authorisation issued.
- Record corrections to time data sheet, if authorisation issued.
- Individual adaptation of authorisations.
- Planning board display: Graphic representation of authorised half-day or whole-day periods of absence in the past and into the future.

Option 5

Type: Visitor management software license.

- Registration of visitors by employees using the Web Client ESS.
- Pre-registration of visitors via Web Client, including entry of additional information for reception staff.
- Automatic forwarding of recorded data to reception staff.
- Display of all personally pre-registered visitors with option of making corrections.
- Availability of data of prior visitors.
- Up to 10 freely definable text fields and up to 5 freely definable checkboxes.

Option 6

Type: System operation general license software license (including unlimited number of administration stations, Web Client supervisors and Web Client ESS).

Requirement: Include the following functionalities:

- Data entry, monitoring and system operation using a standard PC with a Windows operating system (e.g. XP/Vista).
- Compatibility with PCs in the existing work environment.
- Option to define user-group specific views, for relevant data in the Dialogs/Web Clients.
- Option to access customised reports (evaluations) directly from a workstation.
- Option to export reports as PDF and Excel files.
- Language-independent operation of keyboard commands possible (hotkeys) option.
- Language definable for each user.
- Dialog software available in multiple languages (German, English, French) and additional languages (Mandarin, Japanese) if required, i.e. access data from several countries in different languages in parallel.

Adjust language requirement as necessary.

- Easy-to-use on-line help/user manual.
- Call logbooks via Web Clients, with the option to set profiles defining which users may view which logbooks.

Performance features

All dialogs are Unicode-capable.

Single Sign On (SSO).

Communication with database server / Ethernet web server (TCP/IP).

Operating system: Windows Vista, Windows XP, Windows 2000, Windows 2003 Server.

Uses standard web browsers (e.g. Microsoft Internet Explorer or Firefox) to utilise Web Clients on a workstation.

Integrated authorisation check at the start of the dialog.

Number of interactive workstations: Unlimited (simultaneous access from up to 100).

Interactive workstations, minimum requirements for on-site PC:

- Communication with database server: Ethernet (TCP/IP).
- Operating systems: Windows Vista, Windows 2000 Professional, Windows XP Professional.

Hardware (minimum requirements):

- Desktop housing CPU Pentium IV 2.8 GHz 1 GB of RAM.
- Fast Ethernet 10/100/1000 LAN network card.
- HD 40 GB ATAPI CDROM, FDD.
- Free PCI slot and interrupt for video board.
- PCI VGA card with DirectDraw support.

Customised web client extensions

Selections: Kaba exos 9300.

Type: Customised implementation.

Requirement: Include the following functionalities:

- Implementation of third-party applications with the same appearance.
- Integration of customised applications using the Web Client so that they look the same as the access management system.
- Flexible and extendable navigation menus for access management extensions.

Tenant management

In a shared access management system, all tenants can manage their own data and access authorisations with complete autonomy. A software-based tenant management solution is fully integrated in an on-line access management system.

Selections: Kaba exos 9300.

Type: Tenant management software licence.

Requirement: Include the following functionalities:

- Autonomous data management and access authorisations by all tenants.
- Branch mapping through an independent organisation.

Applicable to larger companies.

- Independent service of several customers with a single management system.

For example, security firms, office or technology parks, property managers. Significant cost savings may be possible compared with individual installations through the use of a shared infrastructure (e.g. investments in IT infrastructure, software costs, maintenance, personnel costs.

- Central and individual management of shared services.

For example, authorisations for cleaning and security staff, shared reception, visitor management, parking management.

- Division of building infrastructure responsibilities according to tenants' needs.

For example, peripheral supervision by tenant or central supervision, individual or shared response to alarms, connection to higher-level control centre.

- A grouping mechanism to implement boundaries between different areas of responsibility.

For example, different data access arrangements for different groups based on the company's hierarchical structure.

Performance features

Multiple administration areas per tenant.

Type of tenant:

- Central company system (e.g. tenants in office parks with shared entrance area, e.g. with shared visitor management).
- Separate application service provider (ASP) system (companies with independent divisions/branch offices, i.e. all tenants manage their own active services such as parking management, alarm control centre).
- Mixed systems.

Jointly used access grids (e.g. main entrance).

Complete separation of user authorisations, users, data, access authorisations, logbooks and peripherals from other tenants in the system.

Media - Badge management

Badge management allows mapping of the structure of a physical badge in the access management system. A badge with one designation can contain several media types (5 maximum). This allows a badge card to contain both an inductive badge and a LEGIC badge, for example. The different media types can also have different media numbers, making them completely separate from each other, even though they are physically combined on the same badge card. With this option, badges and media numbers are managed separately from the staff master data.

Selections: Kaba exos 9300.

Type: Badge management software license.

Option 1

Type: Visitor management software licence.

Description: Visitor badge management separate from staff master data.

Option 2

Type: CardLink software licence.

Description: Creation and management of service badges to block specific badges in stand-alone components.

Option 3

Type: B-Net 9107 desktop reader.

Description: Easy search/allocation of LEGIC badges with a desktop reader at the user terminal.

Requirement: Include the following functionalities:

- A combination of different badge technologies, media types and badge structures in one module for parallel use (e.g. LEGIC, Mifare, HID, Hitag, Desfire, STId).
- Assignment of multiple active badges (media) to one person.

For example, one badge permanently installed in a vehicle for access to the parking lot.

- Blocking of all active badges of a person in a single step.
- Permit a different media definition, permittable for each access control hub (substation).

For example, an older building with existing induction readers and a new build with RFID media.

- Transition badge management: Transfer all authorisation data (including authorisation data for stand-alone components and T&A data) on an active badge to a transition badge. When a transition badge is issued, block the main badge immediately.

For example, if an employee forgets their badge, reception will issue a transition badge for one day.

- Automatic replacement of old badges: Issue new badges (badges already initialized in the system) without two badges being valid at the same time. As soon as the new badge is booked for the first time, automatically deactivate the old one in the system.
- Badges with special functions: A specially labeled badge can trigger a particular event.

For example, a booking with this badge activates an alarm system).

- Blocking specific badges in stand-alone components.
- Block/delete all badges held by one person.
- Reliable management of lost, blocked or invalid badges.
- Printing of a receipt when a badge is issued.
- Logging of all changes affecting a badge.
- Badge and badge number management separate from staff master data.
- Search and filter functions for all relevant data.

Performance features

- Badge evaluation according to company code and/or badge number as well as the unique LEGIC number and LEGIC Access™ (structured and unstructured badge data).
- Number of possible media per badge/key: 5.
- Total possible media in access management system: 8.
- Size of badge logbook: Unlimited.
- Media types: LEGIC, Mifare, HID, Hitag, Desfire, STId, etc.
- Badge technologies: RFID, inductive, magnetic strips, etc.

Media - Badge production

A client-server-capable, fully integrated interface for a badge production system operated by VPS in Germany.

Selections: Kaba exos 9300.

Type: KabaCard software license.

Requirement: Including the following functionalities:

- Recording, display and saving of passport photos, signatures and biometric data, automatic image enhancement.

- Display and printing of badges.
- Coding of media types.

LEGIC, MIFARE, HITAG, Chip, etc.

- Design of badges and definition of types.
- Demonstration version.

Media - Programming LEGIC badge segments

Selections: Kaba exos 9300.

Type: Programming of additional segments software licence.

Also required:

- Badge management software licence.
- B-Net 9107 desktop reader.

Requirement: Provide a software-based solution for programming badge segments that is fully integrated in an on-line access management system and includes the following functions:

- Programming of the following segment types on new or existing badges:
  . Kaba Group Header (including programming of media number).
  . LEGIC access (including programming of media number).
  . LEGIC biometric.
  . CardLink.
- If an existing badge is activated subsequently for the purpose of transporting authorisations (e.g. CardLink), automatic registration of whether the necessary segment is already present on the badge. If not, automatic programming of the segment to the badge automatically (kiosk solution).

Access control module

Access control systems enable users to organize complex flows of personnel traffic, create different security zones and record access events and alarms in real time. These multiple requirements can only be met by an integrated module that is part of a new-generation, all-round solution.

Selections: Kaba exos 9300.

Type: Software licence for 4 access points.

Number of access points: Select from 4, 8, 16, 32, 64, 128, 512, 1024, 2048 or more on request.

For operation of multiple access points with identification (1 or 2 registration units/readers connected per access point). Access points without identification do not require a software licence.

Definition of security zones and access authorisations: Provide an integrated module including the following functionalities:

- Protection of people, property and information from unauthorised access.
- Tool for organisational and management of operational processes.
- Division of the corporate structure into various security and administration zones with multi-level security.

Multi-level security concept e.g. North building, London headquarters.

- Central control issue and monitoring of all access authorisations for the on-line system, non-wired stand-alone system components and mechanical locking cylinders.

Based on the security concept of a facility.

- Subdivision of security zones into sub-areas/groups consisting of one or more rooms which may have more than one access point (entrance or exit).

For example, production area.

- Grouping of people so that access authorisations (access profiles) can be issued in line with organisational structures.

For example, production group.

- Assignment of personal access rights, with time restrictions if necessary.

For example, production manager.

- Flexible definitions of access authorisations time.

For example, 7 am midday and 1 pm - 6 pm.

- Additional authorisation checks: Allow with profile-controlled verification e.g. PIN code, biometrics or weight comparison, at freely definable times and only for certain people via a Web Client.

For example, field sales advisors can only access the building after 7pm with a PIN code.

- Depending on the security level, access authorisation to defined areas for certain people.

For example, in the case of a hold-up only security personnel have access to the vault.

- Option to define the parameters of access to controlled areas using drag-and-drop in an intuitive graphic user interface.

The who, when, where and how of access.

- Graphic display of time definitions.
- Filter functions to facilitate searching for/issuing suitable access authorisations.

Performance features:

Access control:

- Number of administration areas: 256.
- Number of persons: Unlimited.
- Number of rooms: Unlimited.
- Number of access grids: Unlimited.
- Number of time zones: Unlimited.
- Number of access profiles: Unlimited.
- Number of access points: Unlimited.

Access point management

No matter whether an access point is a simple door or a complex isolation system, the integrated access point management must allow all components to be precisely coordinated with one another. Access point management must enable operation for a defined number of access points with identification.

Access point management: Coordinate a defined number of access points with identification and include the following functionalities:

- Different door configurations.

Such as simple doors, turnstiles, interlocking door functions with/without integrated scales, etc.

- Integration of all door components.

For example, identification device, verification device, display, keypad, buttons, door opener, door frame contacts,, deadbolt contact, motor lock, etc.

2.3 ACCESS CONTROL STANDARD FUNCTIONS

Alarm handling

Requirement: Include the following functions:

- General and personal alarms: Logging in both the alarm logbook and an alarm handling system. Assign a measures list/checklist to each alarm to help the operator take the appropriate steps if necessary.
- Make alarm handling immediately visible and audible from any dialog. Display active alarms visually on the monitor while an audible alarm sounds.
- At the same time, trigger a number of user-defined actions e.g. trigger door opener, trigger exit controlling a CCTV camera, forward event to a management system.

Optional in combination with the interactive graphics application software module

An interactive graphics application must allow alarm statuses to be displayed in real time on a graphic interface and datapoints (physical devices) to be operated manually with ease.

Automatic badge blocking

Requirement: Provide automatic badge blocking if the wrong PIN code is entered multiple times (defined by the operator).

Opening with badge number

Requirement: For specific, non-security-relevant applications, allow access by entering the badge number on the access reader's keypad.

User roles

Requirement: To prevent an operator from gaining access to unauthorised data, define user roles and entitlement to use elements of the access system. Assign the relevant user role on registration of user name and associated password for every person entitled to operate the system.

Biometric verification

Additional authorisation: Use profile-controlled verification to carry out an additional authorisation check with biometrics at freely definable times, and only for certain people.

For example, access to lab with biometrics only.

Anti-pass back

Requirement: Provide an anti-pass back function to prevent several people from entering the same room or area one after the other by passing on a single badge.

Pass control

General: Whenever access is granted, use appropriate measures (such as barriers, contact mats, isolation) to check whether a person has actually passed through and record a notification in the alarm logbook (passage not completed) or the access logbook (passage completed).

Blacklist

Blacklisted persons: Automatically check all new personal data records (saved or imported) for blacklisting. Save the reason for blacklisting in the system and release blacklisted persons by a special user authorisation only.

For example, if a visitor or contractor data record is being saved to the access management system for the first time, it is automatically checked to determine whether this person has been blacklisted (e.g. as a previous employee).

In/Out control

Requirement: Provide in/out control to prevent a person from entering an individual access grid in which an authorised person is already known to be present. Use identification units in each direction of access, into and out of an access grid.

Annual calendar/Exceptional days

Requirement: Provide for entry of exceptional days, on which access authorisations deviate from the usual pattern in an annual calendar. Make provision for at least 8 different special days of this type, each of which can occur several times within one year. Treat them like additional days of the week in the access profile. Make a distinction between global and local exceptional days. Only allow for assignment of global exceptional days by using by special user authorisation.

Elevator/Lift control (barrier control)

There must be elevator/lift control to control and monitor all instances of access to the various floors of a building complex.

Selections: Kaba exos 9300.

Type: Software licence for 4 access points including Kaba exos AMC Flash E.

Edit number of access points as required. Select from 4, 8, 16, 32, 64, 128, 512, 1024, 2048.

Requirement: Provide elevator/lift control with the following functionalities as part of the integrated access management system:

- Storage of access authorisations for individual floors in the personal authorisation database in the central access management system.
- As soon as a user has registered at the registration unit/reader on the elevator/lift, enable the corresponding floor buttons on the elevator/lift control keypad for a specific period of time, conforming to the user's access rights, to give access to the corresponding floors.
- In addition to elevator/lift control, use the same mechanism to give individual access to cabinets.

For example, lockers at a university, mailbox control.

Bag check (Random rejection)

For the purposes of random control of persons, a random generator must pinpoint a person who can be checked by a member of security personnel.

Selections: Kaba exos 9300.

Type: Software licence for 4 access points including Kaba exos AMC Flash E.

Edit number of access points as required. Select from 4, 8, 16, 32, 64, 128, 512, 1024, 2048.

Requirement: Include the following functionalities as part of the integrated access management system:

- Configuration of a value N for each exit so that using a random generator with Gaussian distribution, the person is blocked until the security check is completed.
- Temporary blockage of the person at all exits in the zone, or flexible configuration of access points.
- Removal of the block by the security officer after the bag check has been carried out on the randomly selected persons.
- Logging of all security checks.

Logbooks

Requirement: Include the following functionalities:

- Access logbook: Automatic entry of all events, including instances of access and rejected attempts at access, where they can be viewed at any time.
- Alarm logbook: Automatic entry of unauthorised access attempts and appropriate accompanying information. Provide for visibility of unauthorised access in alarm handling.

For example, badge unknown or incorrect access grid/time zone.

- Access, T&A, error and alarm logbooks: Show only data for which the user has appropriate authorisation.
- Logbook data: Provide for the following:
  . Real time view of data.
  . Search function for events within a period of time or for specific event types.

Two persons (Four-eye) check

Requirement: Viewing of defined logbooks only by two authorised persons who are present at the same time.

For example, works council member and security officer.

MS Office integrations

Requirement: Provide a system which supports the following tools for the office environment:

- Export staff and logbook data in MS Excel format and for generation of customised reports, diagrams and statistics.
- The Crystal Report program.

Minimum/Maximum control of persons

Requirement: Provide the following functionalities:

- Definition of the minimum and maximum number of persons entitled to be present in individual access grids at any one time.
- When the maximum is reached, blocking of the access grid by the access control reader.
- When the minimum is reached, prevention of the entry or exit of an individual person unless another authorised badge is booked immediately.
- Monitoring of the passage data record to make sure the control is functioning. Isolation is also required.

Office functions

Requirement: Provide the following:

- General office function: Release doors with the first authorised booking of the day and block again with the second authorised booking.

For example, for staff office.

- Personalized office function: Release doors with the first authorised booking of the day and block again with the second authorised booking, but only for defined persons.

For example, seminar leader.

- Assignment of authorisation temporarily to selected individual badges.
- Link with time windows and profiles.

PIN Code Verification

Requirement: Provide for additional authorisation checks. Allow with profile-controlled verification e.g. PIN code, biometrics or weight comparison, at freely definable times and only for certain people.

For example, field sales advisors can only access the building after 7pm with a PIN code.

Optional in combination with the Web Clientsoftware ESS module

Requirement: Issue/change PIN codes on an individual basis via a Web Client.

Opening with PIN Code

Requirement: Provide for the following:

- Individual requirement to enter a PIN code as additional identification.
- Temporary configuration of a PIN code reader to allow access by PIN code only, without the use of a badge. Activation and deactivation of this feature by authorised card holders using the PIN code reader itself.

Room monitoring

Requirement: Provide for entry into predefined rooms in a certain order.

Room and person balancing

Requirement: Provide for querying, at any time, the number of people currently in a defined access grid.

The maximum (and minimum) number of people permitted in a room at any one time must be defined (e.g. capacities for stadiums are defined on the basis of security technology standards).

Roll call

Requirement: Provide for identification, at any given time, of who is present in a defined access grid during an emergency situation using remote access via Web Client.

Interlocking doors

Requirement: Provide for several access points to form an interlocking door to ensure that only one access point can be opened at a particular time or that only one person is inside the interlocking door area.

Weight-based interlocking door option

Include the following text:

Selections: Kaba exos 9300.

Type: Software licence for defined number of access points and Kaba exos AMC Flash E.

Requirement: Provide a weight function to the interlocking door control.

Duress alarm

Requirement: Provide for a definable personal code to trigger the duress alarm. If entry is forced under duress, provide for a certain incorrect code to trigger a silent alarm, grant access as normal and show alarm message on the interactive workstation, but not at the scene of the incident.

There may also be a delay before access is granted.

Code: Make the duress code freely definable.

Two-person access control (Dual verification)

Requirement: Provide for permission to enter/exit defined rooms if two people have proved their access authorisation within a defined period.

Certain rooms cannot be entered alone e.g. the vaults of a bank.

Day/Night operation

Requirement: Provide for release/blocking of access/alarms for certain times and for days/nights using time profiles.

For example, sensors near a door can be deactivated at certain times and cameras and alarm forwarding during the night only.

Scheduler function for the door open profile

Requirement: Provide for planning of the automatic control of the door open profiles in advance.

For example, for holiday times in schools, company holidays.

Event-oriented hardware and software actions/commands

Requirement: Provide a structure for specific software applications/executions/commands with the following functions:

- Program execution (batch file) on the basis of a certain event or alarm in the access management system and transfer of various parameters to this software application.
- Automatic activation/deactivation of binary outputs in the access management system based on a certain event or alarm.
- Automatic generation of emails/SMS messages based on a certain event or alarm.

Datapoint server interface to another system

Requirement: Provide a customised interface between the access management system and a higher-level facility management system with the following functionalities:

- Integration of the access management system in existing facility management systems.
- Transmission of alarms, events and certain data to the facility management system.
- Support of authentication and logging in the audit logbook.
- Forwarding of access control commands and general control commands from higher-level system to the access management system.

Database integrations/Expansions

Selections: Kaba exos 9300.

Type: Kaba exos 9300 Basic System.

Optional Type: CardLink software licence.

- Transport of authorisations to the medium.

Requirement: Provide a customised integration of the access management system database with the following functionalities:

- SQL and Oracle® tools for exchange/integration of data.
- Import of data from existing and/or external systems.
- Support for export of data to other systems.

On-line and stand-alone components

Requirement: Provide a software-based solution that consistently combines and integrates the following system approaches:

- On-line access management system.
- Mechatronic locking system (non-wired access points with stand-alone components).

Functionalities: Centrally implement the following functions:

- Commissioning and administration of the entire system via a common management system. Provide for opening and configuration of both on-line and stand-alone components in a single program so the data is entered once only.
- Complete integration of the programming device for the initialization and programming of stand-alone components.
- Management of all access authorisations from a central point. Continuous documentation of currently valid authorisations throughout the system for all users.
- Full reconstruction of all access and security-related events and recording of all actions (on-line and stand-alone components, programmers) and transfer to the central management system.
- Subdivision of the complete system into administration areas so that a system officer can issue authorisations autonomously within one administration area.

For example, several branches of one company.

- Adoption of the configuration file of an existing mechatronic locking system.

Performance features

Administration areas per system: 246.

Stand-alone components per administration area: 4000.

Stand-alone components:

- Kaba star product family.
- Kaba elolegic product family.
- Kaba elo Programmer 1364 ELC/ELX.
- Configuration file: KIF.
- Medium: LEGIC.

2.4 ACCESS MANAGEMENT SYSTEM - OPTIONAL ACCESS CONTROL MODULES

Visitor management

Visitor management allows all visitors to be easily recorded, organised and monitored from pre-registration with a Web Client to the return of a badge when leaving the building.

Selection: Kaba exos 9300.

Type: Visitor management software licence.

Optional:

Type: Kaba Card software licence (include ID Expert SDK components from VPS).

Includes the following functionalities:

- Take visitor photograph.
- Print visitor badges.
- Design visitor badges (different layouts must be possible).
- Code visitor badges.

Type: Badge management software licence.

Includes the following functionalities:

- Issue/return (assign) predefined visitor badges in badge management.

Type: Parking management software licence.

Includes the following functionalities:

- Check visitors in and out in parking management.

Type: Web Client ESS software licence for a defined number of persons.

Includes the following functionalities:

- Web Client for registering visitors.

Type: Tenant management software licence.

Includes the following functionalities:

- Tenant-enabled visitor management.
- A tenant can transfer the management of their visitors to another tenant (e.g. responsible tenant at reception desk).

Type: Software module Customised integration of visitor cards and ID readers.

Includes the following functionalities:

- Automated recording of visitor data or quick registration at reception.

Type: B-Net 9107 desktop reader.

Includes the following functionalities:

- Automated, easy registration and check-out of badges (visitors) using a desktop reader at the user terminal.

Requirement: Provide a software-based visitor management solution that is fully integrated in an on-line access management system and includes the following functionalities:

- Pre-registration of visitors and simplified registration process for previously registered visitors.
- Recording of detailed visitor data, including photo (e.g. surname, first name, company, address, staff ID, vehicle details, etc.) by means of adaptable data input menus (assistants, wizards).
- Recording details of person receiving visitor (including name, telephone number, department).
- Web Client for registering visitors.
- Additional, freely definable, customised fields.
- Customised data input processes using wizards.
- Issue visitor pass and/or visitor badge using different layouts, if required.
- Individual access authorisations for (pre-registered) visitors or groups of visitors, and simple appointment rescheduling.
- Automatic invalidation of the badge after termination of the visiting period or upon surrender of the badge.
- Automatic check-out of the visitor at defined readers (e.g. Kaba Card Collector CRP-M01).
- Automated registration and check-out of visitors' badges using a USB desktop reader
- Visitor status known at all times.

Where is a visitor and who are they with?

- One click booking in and out of persons registered in visitor management. Automatic modification of the current occupation in parking management when a booking is made.
- List of all blocked visitors (blacklist).
- Logbook of all visitor movements inside a building.

- Search function for all relevant data.
- If a member of staff has forgotten his or her badge, assignment of a transition badge using the visitor management module. Automatic transfer of authorisations for time and access booking and blocking of the standard badge.
- Support of multiple branches of one company through a grouping function, with filter function for all relevant visitor data for a given branch and flexible user authorisations for each group/branch.
- Tenant system: Transfer of the management of individual tenant visitors to other tenants.
- Data deletion interval: Freely definable time after which all visitor data is deleted from the database.
- Multiple language versions.

For example, a different language per branch.

Contractor management

Selection: Kaba exos 9300.

Type: Contractor management software licence and Administration station software licence for 1 operator.

Edit to suit the number of operators. Select from 1, 3, 6, 10, 30, 60.

Optional:

Type: Software licence for a defined number of persons for time and attendance.

- Integrated time and attendance for contractor employees.

Type: Personal notification AC software licence.

- Safety check with expiry date and automatic personal notification.

Type: KabaCard software licence.

- Create contractor employee badges.

Requirement: Provide a software-based contractor management solution that is fully integrated in an on-line access management system and includes the following functions:

- Integrated administration of all master data relating to a contractor and the contractor's employees.
- Integrated administration of all rights of a contractor and the contractor's employees.
- Registration and management of projects.
- Audit procedure: Logging relevant events in a logbook.
- Linking of contractor employee access rights to the project duration.
- Linking of contractor access rights to the validity of a safety check and work permit.
- Automatic personal notification before expiration of a safety check or work permit.
- Definition of the period of validity of the certification of a contractor, evaluations of security and invoice-related processes, and generation of a message on expiration of validity period expires.
- Automatic evaluation times by project, create reports and analyses with the required data, and to forward these for invoice checking.
- Issue a of work bans.
- Administration/operation using Web Client.

Transport of authorisations on the medium (CardLink – Type)

Selection: Kaba exos 9300.

Type: CardLink software licence and the following:

- Badge management software licence.
- Stand-alone components:
  . Kaba elolegic c-Lever CardLink(TM).
  . Kaba elolegic digital cylinder CardLink(TM).
  . Kaba elo Programmer 1364 ELC/ELX.
  . Configuration file: KIF.
- Medium:
  . LEGIC prime, MIM 256 or MIM 1024.
- Update function:
  . Kaba exos iDML, USB desktop reader B-Net 9107, Bedanet 93 xx.

- Validation function:
  . Kaba exos iDML, Kaba exos cDML, Kaba exos DML2, Bedanet 93 xx.

Options

Type: SW licence Web Client for a defined number of supervisors (1, 3, 6, 30, 60, 100, 300).

- Update of the CardLink authorisations for all employees.

Type: Personal notifications software licence.

- Automatic sending of a request by email to the respective employee to update the CardLink authorisations.

Type: SW licence programming of additional segments. Existing badges can additionally be programmed with the following segment types:

- Kaba Group Header (including programming of the media number).
- LEGIC access™ (including programming of the media number).
- LEGIC Biometric™ - CardLink™.

Also required:

- SW licence badge management.
- USB desktop reader B-NET 9107.

Requirement: Provide a software-based solution that is fully integrated in an on-line access management system and includes the following functions:

- Management of all access authorisations from a central point, continuous documentation of currently valid authorisations throughout the system for all users and reconstruction at any time.
- Saving of the personal authorisation data for stand-alone components directly on the secure RFID medium.

These authorisations must be read by the stand-alone components on site and evaluated for an access decision. A validation mechanism additionally checks whether these authorisations are valid.

- Operational reliability including the following:
  . Set the validation period individually, depending on security requirements.
  . After expiration of validation period, invalidate the data on the badge.
  . If a badge is lost, prevent unauthorised access through active authorisation withdrawal.
  . For immediate blocking, generate a blocking badge.

Only badges with authorisation for a defined time and which are additionally validated are allowed access at the stand-alone components.

- Immediately deletion of validation at certain readers.

For example, exit readers.

- Set the validation period for each component for entrances that are not relevant from a security perspective independently of the personal validation period.

For example, parking barriers. Access at these access points is also possible following longer absences, such as holidays or weekends. If individual access rights need to be updated, this must be signalled to the user. Updating must be performed in a user-friendly way at a special on-line reader. There must be additional mechanisms to cope with everyday situations, such as lost or forgotten staff badges and the issuing of visitor badges. It should not be necessary for the stand-alone components to be re-programmed on site.

- Modification and validation of access authorisations for stand-alone components at different branches of the same company using an authorisation reader on a Web Client over the company's own intranet.
- Grouping of stand-alone components into door groups which can each be assigned a fixed time zone. Assignment of an access point to more than one door group. Assignment of door groups to persons or groups of persons as a part of an access profile.

For example, production group with time zones 6am to 6pm .

- Assignment of personal access rights including a definable time zone.

For example, production manager has access to warehouse doors between 6pm and 6am .

- Activation of an individual office mode for each badge.
- Locker locks: Support access rights at a specific locker or with free locker selection including the following:

. Except as below, after the locker has been locked with the badge, the locker lock may only be opened with this badge.
. Allow access using a special badge.

For example, for service personnel.

. Define the maximum occupancy period to prevent the locker from being occupied for too long.
. Transfer of status information to the central access control system via media.

- Automatic read-in of unique numbers of existing badges at certain readers.

For instance, where there are multiple locations, the security officers must define and manage their access rights, doors, door groups and time zones completely independently of one another. (Administration areas). Within this context, it must be possible to use a single LEGIC segment for multiple locations (administration areas).

- Programming of the necessary badge segment to the media by system operators using a USB desktop reader or Web Client.

Performance features

Door groups per administration area: 512.

Time zones per administration area: 16.

Time windows per time zone: 7.

Validation periods per administration area: 8.

Door groups per medium: 512.

Individual rights per medium (guideline value): 20.

Status information per medium:

- Battery status alarm for stand-alone component.
- Storage capacity of event memory in the stand-alone component.

Image verification

Selection: Kaba exos 9300.

Type: Manual image verification software licence.

Optional

Type: Software module Customised integration of live image display.

- When image verification is employed, the image of a person stored in the system and the live image of the person is automatically displayed on a second monitor following an authorised or unauthorised access attempt.

Requirement: Provide a software-based image verification solution that is fully integrated in an on-line access management system and includes the following functionalities:

- Multiple-user capable access point monitoring and sequential staff image display.
- Configurable display of staff data and display of all authorisations for the individual.
- Free parameter selection for required access points (doors) for automatic display of photo.
- List of monitored access points/registration units.
- Free selection of next image comparison from a queue.
- Placement of access attempt further down the queue.
- Direct release of the doors from a workstation.
- Parameterisation of image display based on defined events on the reader.

For example, authorised access.

- Parameterisation of image deletion based on defined events.

For example, following manual release of door or after a defined delay.

- Administrator selection of pending access inquiries from a list (waiting queue) and/or of delay access inquiries if multiple administrators are responsible for processing access inquiries.
- Automatic assignment of access inquiries to the administrators: Conform with the following:
- Even distribution: Skip the administrator who processed the last access inquiry.
- Search for the first free administrator for the pending access inquiry.
- Graphic and individually configurable user interface.

- If multiple operators are working at one workstation, tracking of which operator issued which access via identification of the operator badge as a prerequisite to granting access.

Depot control

Depot control allows and efficient control and monitoring of keys and other objects. The depot control comprises one reader and the individual depots. A depot might be a lockable compartment, a mailbox or a cylinder.

Selection: Kaba exos 9300.

Type: Depot control software licence for Kaba exos 9300 plus Kaba exos AMC Flash 2 E for 2 depots.

Connection of up to 2, 4, 6, 16, 32 depots. Edit as required.

Requirement: Provide a software-based depot control solution that is fully integrated in an on-line access management system and includes the following functions:

- Administration and control of keys, repositories and cylinders.
- Monitored, time-controlled issue and return of keys and other objects.
- Stored authorisations for depots in the personal authorisation data in the central access management system.
- Overview of the current status of present and removed depot objects.

For example, keys.

- Parameterisation of a general authorisation for all depots and depot controls.
- Specific logbook for on-line analyses for each depot and person.

Performance features

Number of repositories per depot: Maximum 192.

Types of depot:

- Key issuing devices.
- Key deposit tubes.
- General repositories (e.g. laptops).

Operating modes:

- On-line.
- Off-line up to 7500 events.

Personal notifications by email

Selection: Kaba exos 9300.

Type: Personal notifications software licence.

Requirement: Provide a software-based solution for the automatic sending of email requests that is fully integrated in an on-line access management system and includes the following functions:

- Email to the relevant employee notifying them of the need to update the CardLink authorisations.
- Email to the relevant employee/contractor employee notifying them of the need for safety instructions (safety check).
- General performance: Provide the following:
  . Reports via the Web Client.
  . Definition and completion of reports using special user rights only.

For example, administrators (report definition) and employees (report completion).

- Reports based on a common standard so that no additional licences from third-party providers are necessary.

For example, Microsoft RDLC.

  . Output formats: Adobe PDF or Microsoft Excel.
  . Expanded functions for reports.
- Access: Provide the following:
  . Starting reports from a dialog box.
  . Starting reports independently of the access management system.
  . Automatic starting of reports.

For example, weekly.

. Comprehensive filtering and grouping options.

- Time and attendance: Provide the following expanded functions for time and attendance via Web Client:
  . User-defined reports in tabular form for evaluating time and attendance data.
  . Reports for individual persons or hierarchy levels.
  . Specific authorisation requirements for users to create reports.
  . Output format: Adobe PDF or Microsoft Excel.

Production of customised reports

Selection: Kaba exos 9300.

Type: Extended report function software licence including:

- Crystal Runtime environment for display and printer output.
- Service outlay for production of customised reports based on Crystal Report: Crystal Reports Designer.

Requirement: Provide a software-based solution for customised reports that is fully integrated in an on-line access management system and is based on Crystal Report, and includes the following functions:

- Free design of chosen customised reports with Crystal Report Designer.
- Direct integration of reports in the access management dialogs.
- Direct print-out of reports conforming to authorisations in the access management system.
- Starting reports from various dialogs.
- Starting reports with separate program.
- Automatic starting of reports.

For example, daily or weekly.

- Comprehensive filter and grouping options.
- Various export formats such as Microsoft Excel, Adobe PDF, XML, HTML, RTF.

Parking management

Company parking management allows the following:

- Efficient organisation of spaces.
- Secure monitoring of spaces.
- Evaluation of the suitability of spaces to the individual user.

Selection: Kaba exos 9300.

Type: Parking management software licence.

Optional Type: Visitor management software licence.

Includes the following function:

- Assignment of a visitor parking space.

Requirement: Provide a software-based parking management solution that is fully integrated in an on-line access management system and includes the following functions:

- Individual division of parking lots spaces into parking lot pools based on groups of people or individuals.

For example, visitors, tenants, employees, VIPs.

- Division of parking lots into sectors and levels.
- Flexible administration and assignment of entrance and exit readers.
- Authorisation check based on personal access rights (already stored in the access control system) using access grids and time zones. Limitation of access by individual person and specific period of time.
- Multiple use of a parking lot through evaluation of individual access authorisation for the building (linking of access control and parking lot occupation).
- Consideration of parking lot occupation in group parking lots.

For example, pool parking lots for employees.

- Balancing: On-line information on occupation of parking lots.

- User-appropriate evaluation of actual parking lot usage for individual or flat-rate billing.

Company divisions, profit centres, tenants, etc.

- Logbook listing individual entries/exits.
- An identification medium for both parking lot access and the building.
- Tree view function: A user-friendly graphic overview of all parking lot components (parking areas and parking lot pools).

Mobile phone access identification

Selection: Kaba exos 9300.

Type: Kaba exos 9300 interface to SecLoc software licence and Mohito licence (SecLoc).

Requirement: In addition to the registration units with badge media, enable use of mobile phones for access identification and T&A booking. Include the following functionalities:

- Opening of remote off-site doors without the issuing of badges.
- Granting of access rights and authorisation via the access management system.
- Fit doors with a bluetooth detector if required to check whether the mobile phone is actually next to the door.
- Both SMS and GPRS connections.
- All bookings recorded in the central management system.
- Withdrawal of access rights at any time by the central system.

Master key systems management

Selection: Kaba exos 9300.

Type: Kaba exos software licence for management of mechanical locking systems with up to 250 components.

Kaba exos software licence for management of mechanical locking systems supports 250, 500, 1000, 2000, 4000 or unlimited components. Edit as required.

Optional Type: Kaba exos contractor management.

Includes the following function:

- Registration of mechanical keys held by contractors (e.g. fire department, electricity).

Requirement: Provide a software-based master key systems management solution that is fully integrated in an on-line access management system and includes the following functionalities:

- Central management of mechanical components (locking cylinders, keys), mechatronic components (mechatronic locking cylinders, keys with integrated RFID medium) and on-line components.
- Import and save one or more new or existing master key systems from different manufacturers. Trace which key fits which cylinders.
- Management of all media, including keys, within a single system and assignment to individuals.
- Availability of overview of all the authorisations for a person at all times.

That is, where a person has access, when and with which medium (key).

- A key plan view for a master key system or person.
- Display user keys and locking cylinders in conformance with their needs.

For example, by floor, building or location.

- Display option for keys not returned on time.
- Restriction of visibility and access protection by master key system and location.
- Process-oriented support for the issuing and return of keys (may be several keys at the same time), including automatic creation of relevant receipts and lists.
- Transaction record and tracking of who was given which key and when.
- Deposit administration.
- If on-line access authorisations are blocked, notification of the security service of the need to recover the keys.
- Regular checking of the stock of keys.
- Reporting function supporting evaluations based on persons, keys, access authorisations, access points, key closing functions or scheduled return deadlines.

- Export function for the key plan.

Performance features:

Supports manufacturer-neutral industry standard KWD (KeyWorlD).

Customer-specific integration of additional data formats.

Mechanical locking system:

- Any manufacturer.
- Unlimited number of locking cylinders and keys.

All security-relevant actions must be logged in the management system (system logbook, badge logbook, alarm logbook, audit logbook)

OPC Interface to higher-level facility management system

Selection: Kaba exos 9300.

Type: OPC Server software licence plus service outlay for customised integration.

Requirement: Provide a standardized OPC interface between the access management system and a higher-level facility management system that includes the following functionalities:

- Interface validity for all tenants in the system.
- Integration of access management system in existing facility management systems.
- Transmission of alarms and events to the facility management system.
- Forwarding of access control commands and general control commands from higher-level system to the access management system.

Interactive graphics application

Selection: Kaba exos 9300.

Type: Interactive graphics application software licence.

An interactive graphics application allows display of alarm statuses in real time on a graphic interface and easy manual operation of datapoints (physical devices).

Requirement: Provide a software-based graphics application solution that is fully integrated in an on-line access management system and includes the following functionalities:

- Interactive, graphic overview of the status of the entire system periphery, intuitive and in real time (tree view).
- Hierarchical representation of building structure.
- Multiple graphic overviews in one system.
- Interactive operation of datapoints (access points, binary contacts).

For example, open doors once or activate/deactivate cameras with a click of the mouse.

- Alarm management with automatic navigation to associated building view.

For example, door open alarm on 12th floor.

- Direct alarm handling with a click of the mouse.
- Checklists for operators: Individually displayed in the event of an alarm and listing the measures to be taken.
- Freely available library with ready-made pattern (icons) to represent statuses.

For example, lamp, camera, etc.

- Simple configuration of the graphics with drag-and-drop.
- Automatic generation of page and datapoint hierarchy.
- Real-time interface for forwarding of events and alarm messages as well as movement data via TCP/IP.

Performance features

- Number of graphic overviews per system: Unlimited.
- Number of datapoints: Unlimited.
- Operating modes: Operator mode and draft mode.
- Statuses: Alarm status acknowledged (confirmed) and alarm status not acknowledged (flashing).
- Library of icons: Freely extendable.
- Graphics formats: BMP, GIF, JPG, WMF, EMF.

- Real-time interface format: XML.

LDAP connection

Selection: Kaba exos 9300.

Type: Kaba exos 9300 software licence for LDAP connection for 250 persons plus service outlay for customised integration.

Connection for up to 250, 500, 1000, 3000, 10,000, more than 10,000 on request. Edit as required.

Requirement: Provide a standardized protocol that includes the following functionalities:

- Lightweight Directory Access Protocol (LDAP) connection to an access management system and directory services on the customer side with a defined number of persons.
- Simple opening of new persons by data import.
- Import of staff data in the access management system with the data in the central directory service.
- Alignment with several directory services.

Interface to SAP ERP HCM / KK1 / HR PDC

Selection: Kaba exos 9300.

Type: Kaba exos 9300 software licence TR for ERP HCM for up to 250 persons.

Licence available for up to 250, 500, 1000, 3000, 10,000 persons. Edit as required.

Requirement: Provide a certified interface between the access management system and mySAP ERP HCM that includes the following functionalities:

- Efficient data processing: Record all staff data only once and automatically transfer to the other system to avoid duplicated data storage.
- When networked with SAP R/3 HR Time, management and control of the whole periphery by the access management system.
- Forwarding of logged bookings directly to SAP ERP HCM.
- If an employee forgets their badge, issuing of a replacement badge by the local access management system without having an impact on the function of the overall system. Automatic transfer of all access rights to the replacement badge.
- For temporary employees, visitors (or visitor parking lots) and contractors' employees management directly with the access management system at a local site, independently of SAP.
- Support of full tenant function so that the interface can be used by several companies at different locations.
- Certification: Provide evidence of vendor certification for the open application and integration platform SAP NetWeaver.
- Option for using the interface for customised integrations of T&A systems.

Time and attendance

T&A systems must meet very high requirements. All the time data they contain must be coordinated efficiently and precisely to different working time models. It must be also be possible to transfer data to the payroll system of choice. There should be a variety of evaluation options to provide useful management information. It must be possible to use time & attendance terminals for access control as well, including the combined display of time & attendance or SAP and access texts. There should be a variety of evaluation options to provide useful management information.

Selections: Kaba exos 9300.

Type: Time & Attendance software licence for up to 100 persons.

Available in steps of 100 or 1000. Edit as required.

Optional items

Type: Option package software licence:

- Including 1 Transfer program software licence.
- Including 1 Cost centre accounting software licence.
- Including 1 Mass time and quick correction software licence.
- Including 1 Personal notifications software licence.
- Including 1 Standby accounting software licence.

Type: Tenant management software licence:

- Tenant-enabled time & attendance.

- In a tenant system the number of persons is divided between the tenants.

Requirement: Provide a software-based T&A solution that is fully integrated in an on-line access management system and includes the following functionalities:

- General T&A functions:
  - . Central staff master data with comprehensive data and displayable image of person combined with access control.
  - . Dialog integrated into the staff master data for correction of all necessary time data.
  - . Company hierarchies.
  - . Branch support.
  - . Calendar for defining various exceptional day groups.
  - . Planning board for graphic display, entering and correction of absences, with individual colour assignment for time types.
  - . Automatic calculation of holiday entitlement for new employees.
  - . Entry of hourly absences (time).
  - . Date-related change of time model and hierarchy.

For example, during reorganisation or changes in department.

  - . Automatic checking of legally stipulated shift sequences including compliance with mandatory company holidays.
  - . Individual rounding for each work profile.
- Time definitions:
  - . Definition of work models by utilisation of time types, absence definitions, time ranges and work profiles.
  - . Configurable absence, bonus and overtime definitions.
  - . Stipulation of daily, monthly and yearly quota working times.
  - . Rest period monitoring.
  - . Advance planning of periodically recurring and known absences.
  - . Automatic accounting of all entered time registrations, corrections and planned absences.
- Evaluations:
  - . Printing of error lists to determine time corrections.
  - . Printing of time data sheets as staff information and management tool.
  - . Absence overviews, daily bulletins, monthly and yearly statistics.

Configurable Transfers

Selection: Kaba exos 9300 with Transfer program software licence.

Requirement: Provide a software-based additional T&A solution that allows configurable transfers for periodic implementation.

For example, daily, weekly, monthly, and yearly.

Cost Centre Accounting

Selection: Kaba exos 9300.

Type: Cost centre accounting software licence.

Requirement: Provide a software-based additional T&A solution that allows cost centre accounting and includes the following functionalities:

- Registration of cost centre times per person.
- Evaluation per person and company hierarchy, total worked time per cost centre over a given period.
- Evaluation per department and company, total worked time per cost centre over a given period.
- Change between cost centres on T&A terminal.

Mass time and quick correction

Selection: Kaba exos 9300.

Type: Mass time and quick correction software licence.

Requirement: Provide a software-based additional T&A solution that allows corrections to a group or all persons and offers the following functionalities:

- Fast registration and booking of several time corrections for each person with special dialog.
- Collected registration and booking of a time correction for each group of persons with special dialog.

Personal notifications by email

Selection: Kaba exos 9300.

Type: Personal notifications software licence.

Requirement: Provide a software-based additional T&A solution that allows for the automatic sending of an error log in the event of erroneous time data.

For example, forgotten coming / going booking, absence without reason, and violation of core time.

Standby Accounting

Selection: Kaba exos 9300.

Type: Standby accounting software licence.

Requirement: Provide a software-based additional T&A solution that automatically handles bonus calculations for standby operations.

T&A Functions for employees

Selection: Kaba exos 9300.

Type: T&A functions for employees software licence with Web Client software licence for employees.

Number of employees: [complete/delete]

Indicate the actual number, a maximum or as documented.

Requirement: Provide a Web Client-based solution for employees that can access various T&A functions individually and includes the following functionalities:

- Display time data sheet.
- List of absentees showing reason for absence.
- Record coming/going (with reasons) if authorisation issued.
- Record corrections to time data sheet, if authorisation issued.
- Option to adapt authorisations individually.
- Planning board display: Graphic representation of authorised half-day or whole-day absences in the past and into the future.

T&A functions for supervisors

Selection: Kaba exos 9300.

Type: T&A functions software licence for supervisors plus Web Client software licence for supervisors.

Number of supervisors: [complete/delete]

Indicate the actual number, a maximum or as documented.

Requirement: Provide a Web Client-based solution for supervisors that can access various T&A functions individually and includes the following functions:

- Time data sheet display and corrections of assigned employees.
- Signature function for employees and supervisors.
- Planning board display: Graphic representation of approved half-day or whole-day absences in the past and into the future, work profiles and error codes.

In the event of violation of core time.

- Integrated workflow for the approval of holidays and other periods of absence.
- Option for the supervisor update to CardLink authorisations for the employees that report to him.

XML interface

Selection: Kaba exos 9300.

Type: Customised integration.

Requirement: Provide option to implement project-specific interfaces for bidirectional data transfer between the access management system or the T&A system (database) and an external system using standardized data (XML).

Software maintenance contract
Selection: Kaba exos 9300.

Type: Kaba exos 9300 upgrade licence/annual fee with option to terminate at the end of a calendar year with a notice period of 3 months.

The software maintenance contract is an agreement between the access management system user and the vendor whereby new software upgrades are supplied free of charge. The access management system must be continually expanded and improved with the latest technologies and offers the system user the following benefits:

- Support of organisational structural changes, e.g. new building infrastructures (e.g. additional branches, extra building with an existing building control centre), staff changes (new positions).
- Use of the latest system functions and the option of using extra software modules, e.g. key system management, contractor management.
- Use of new access management trends (e.g. transport of authorisations to the medium).
- Support of new hardware components, e.g. latest generation of readers or access hubs.
- Support of the latest media technologies and standards (ISO).
- Support of new IT technologies (For example, network technologies, security standards, encryption algorithms, etc.).
- Support of new operating systems.
- Support of new web technologies.
- Support of new database standards and releases (SQL, Oracle, etc.).
- Support of new interface technologies for connecting to external elements (OPC, XML, SAP, etc.).
- Support and maintenance of customised software and special adaptations, i.e. customised software developments must be automatically incorporated in a software upgrade.

2.5 ACCESS MANAGEMENT SYSTEM ARCHITECTURE EQUIPMENT (PCS, SERVERS AND ASSOCIATED IT INFRASTRUCTURE ON SITE)

Database server
Requirement: Provide database server in conformance with the following:
- Databases: Microsoft® MSDE 2000, Microsoft® SQL 2000/2005/2005 Express and Oracle® 9i/10g.
- Support of Single Sign On (SSO) and LDAP connection.
- Not dependent on operating system.

Hardware: Provide minimum requirements as follows:
- High stringency requirements:
  . 19" rack housing.
  . 2 x Intel Xeon® 3.2 GHz processor.
  . 2 GB of RAM.
  . 2 x Fast Ethernet 10/100/1000 network cards.
  . 3 x HD 120 GB SCSI RAID 5, H-Plug.
  . 1 x Smart Array 5i plus controller.
  . 2 x 230 V a.c. mains supply unit, 400 W, H-Plug.
  . ATAPI CDROM, FDD, PCI 2MB graphics chip.
  . UPS as Smart 1000 VA 19" including Power Chute.
- Medium requirements:
  . 19" rack housing.
  . 1 x Intel Xeon® 2.8 GHz processor.
  . 1.5 GB of RAM.
  . 1 Fast Ethernet 10/100/1000 LAN network card.
  . 3 x HD 80 GB SCSI RAID 5, H-Plug.
  . 1 x Smart Array 5i plus controller.
  . 230 V a.c. mains supply unit, 420 W, H-Plug.
  . ATAPI CDROM, FDD, PCI 2MB graphics chip.
  . UPS as Smart 500 VA 19" including Power Chute.
- Low stringency requirements:

. 19" rack housing.
. 1 x Intel Pentium® IV 2.8 GHz processor.
. 1 GB of RAM.
. Fast Ethernet 10/100/1000 LAN network card.
. 2 x HD 60 GB SCSI, mirrored.
. Smart Array 5i plus controller.
. 230 V a.c. mains supply unit, 400 W, H-Plug.
. ATAPI CDROM, FDD, PCI 2MB graphics chip.

Communication hub

Communication with the database server: Ethernet (TCP/IP).

Communication with the access hub/access manager/terminal: Ethernet (TCP/IP), RS-485, dial-up modem.

Communication with the door manager: Ethernet (TCP/IP), encryption possible.

Operating system: [complete/delete]

Select from Options

Windows® 2003 Server

- Standard Edition.
- Enterprise Edition.
- Datacentre Edition.

Windows® 2000

- Professional Server.
- Advanced Server.
- Datacentre Server.

Windows® XP Professional.

Hardware (minimum requirements): Intel Pentium® IV, 512 MB of RAM.

Web Server (WEB-S), Internet Information Service IIS

Hardware (minimum requirements): Intel Pentium® IV, 512 MB of RAM, HD > 50 MB.

Access hub

Communication with communication hub: Ethernet (TCP/IP), RS- 485, dial-up modem.

Door manager (door controller)

Communication with access hub: RS-485.

Ethernet (TCP/IP): Encryption possible.

Extension modules for alarm management

General: Provide extension models in conformance with the following:

- Can be plugged into door manager.
- Up to 16 inputs and 8 line-monitored inputs.

On-line registration units

General: Provide the following:

- Access readers (with PIN code).
- Terminals for operating data and time registration.
- Access readers and terminals for various media: LEGIC, Mifare, HID.
- Flexible reader designs that can be adapted to the building architecture.
- Wide-range solutions.
- Biometric solutions.
- On-line locks and cylinders.
- Depot devices.
- Motorised badge readers.

Stand-alone registration units

General: Provide the following:

- Digital locking units (digital cylinders, panic lock).
- Mechanical locking cylinders.
- Locker locks.
- IT-locks.

Mobile registration units

General: Provide the following:

- Mobile registration readers.
- Mobile phone.

Identification devices (media)

General: Provide the following:

- LEGIC.
- Mifare.
- HID.
- Hitag.
- Desfire.
- STId.

Badge technologies

For example, combi badges and hybrid badges,

Requirement: Provide the following:

- RFID (contactless).
- Inductive.
- Magnetic strips.

Expandability/scalability

Interactive workstations: unlimited (simultaneous access for up to 100).

Web Clients: 10 000.

Communication hubs: Unlimited.

Persons and badges: Unlimited.

Access hubs: 10 000.

Terminals: 10 000.

Access pts (readers/doors): Unlimited.

Standard interface for connecting to external systems

Requirement: SAP KK1, SAP R/3 ERP.

Open interfaces for connecting to external systems

Requirement: Provide the following:

- SQL/Oracle database connection.
- Crystal Report data evaluations.
- XML on-line interface.
- LDAP Active Directory connection.
- OPC server.

2.6 ACCESS MANAGEMENT SYSTEM HARDWARE

Access control hub

The access control hub is used to monitor and control access points and datapoints. A distinction is made between on-line, off-line and remote operation.

In on-line operation, a connection is established with the communication hub (COM hub). The access control hub forwards bookings and alarms to the COM hub. If the connection is interrupted, the access control hub switches to off-line operation and makes access decisions itself.

In off-line operation, the access control hub implements checks and makes decisions on access authorisation by comparing the currently available information from the connected identification registration units with the access authorisation data stored in the access control hub.

For access authorisation, at least the following parameters must be checked:

- System to which identification medium belongs.
- Validity of the identifying features.
- Time-limited access (time zones: days, hours, minutes).
- Space-limited access (access grids).
- Repeat access lock.
- PIN code.
- Biometric verification.
- Seamless logging.

In remote operation, the connection to the system is only established when required. That is, the decision on access and the control of access points is the same as in off-line operation. Communication only needs to be established with the system in the event of alarms and changes in configuration.

Control functions: Provide the following:

- Control of access control elements: Adjust to the duration of control within the range of 1 – 60 seconds.
- When connecting to alarm systems, transfer the alarm data and fault data of the access control system to the alarm system.
- Arming or disarming the alarm system and/or suppress alarm messages from the alarm system in the event of access by authorised persons.
- RS-232 interface for customised integration options.

Monitoring functions: Provide the following:

- Monitoring of access points included in an access control system for opening.
- Monitoring of authorised opening of access points on a time basis (open time monitoring) and adjustment of the permitted open time for each access point within the range of 5 – 60 seconds.
- Continuous monitoring of the housing of the access control hub for opening.
- Internal clock: In conformance with the following:
  . Function: Generation of the current time and date.
  . Time error tolerance: ± 30 seconds over a 30-day period.
  . Time and date synchronization by the access control system.
- Monitoring of the transmission paths between the system components connected to the access control hub to provide reliable transfer of information between these components.

Door monitoring: Provide interfaces for the connection of door monitoring and door control for each connected identification unit.

Customised door management: In addition to access handling, provide option for customised door management functions such as elevator, IDS and interlocking door control functions.

Scalable connection: Allow the scalable connection of up to 32 door managers with up to 64 RFID registration units.

Performance features

Memory capacity per Compact Flash (TM):

- >100,000 persons / badges.
- Logbook for at least 30,000 events (off-line).

Interfaces:

- PC104 controller with integrated Ethernet interface to network connection.
- RS-485/ 2 interfaces.
- 2-wire party line for communication with maximum 32 peripheral devices (maximum 64 access points).
- BPA-9 protocol.
- RS-232 for the customised integration of special applications.

Inputs:

- 4 binary inputs for potential-free contacts, active/inactive (one can be used as tamper switch).
- LED status display active / inactive.

Outputs:

- 3 relay outputs with changeover contact.

- Changeover contact; maximum 2 A at 30 V a.c./d.c.
- LED status display active/inactive.

General:

- Dimensions 400 x 400 x 120 mm (with housing).
- Mounting: wall mounting (with housing) or customised (without housing).
- Operating temperature 0° to +40°C (50°C without external power supply load).
- Protection type: IP54 with housing (optional) and cable connections.
- CE approval.
- Standards: EN 55022, EN 55024, EN 60950-1.

Access control hub selections

Selection: Kaba exos AMCII.

or

Kaba exos in 19" metal rack module.

- 2U 19" metal housing with status display of the inputs and outputs, mains transformer (230V, 1.5 A) and DIN rail for additional terminal strips on rear, IP40.

and

Selection: Kaba exos AMC Flash 2.

Number of devices: Connection of up to 2, 4, 6, 16 or 32 devices to BPA/9 subset. Edit as required.

- Supports CardLink™ **or** Kaba exos AMC Flash 2E.

Number of devices: Connection of up to 2, 4, 6, 16, 32 devices to BPA/9 subset.

- Supports CardLink™, elevator control, depot control, weight-based interlocking door, control of alarm zones (connection to alarm systems).

Option 1

Type: Kaba Metal housing.

Requirement: Metal housing, lockable, with tamper switch, DIN rail and strain relief.

Option 2

Type: Kaba Power supply unit 230 V/24 V 100 VA.

Requirement: 230 V/24 V 100 VA mains supply unit for up to 10 access points.

Optional Extension Unit for Controlling Alarm Zones

Type: Kaba exos PC104 I/O board.

Requirement: Provide an extension board with binary inputs and outputs for the access control hub, which includes the following functionalities:

- Optional addition to access hub for controlling alarm zones.
- Inputs: Line-monitored.
- Access management system: Free use of the inputs and outputs.

Performance features

Connections: Screw terminals.

Mounting: PC-104 interface for direct mounting on the access control hub processor board.

Plug-and-play operation.

8 inputs: Line-monitored (monitored/not monitored can be set by DIP switch).

8 relay outputs:

- Normally open / normally closed contact adjustable with jumper.
- Power consumption 30 V/2 A.

Door manager (Door controller)

Type: Kaba exos DML2.

Option 1

Type: Kaba exos IC8.

Description: Extension module with 8 additional line-monitored inputs.

Option 2

Type: Kaba exos OC8.

Description: Extension module with 8 additional outputs. 2 extension modules possible (total of 16 additional outputs).

Requirement: Provide door manager which works with remote RFID registration units (antennas, PIN code, biometrics, on-line locks and cylinders) and in combination with contactless RFID technology such as LEGIC and other ISO standards, and includes the following functionalities:

- Installation in a tamper-proof place irrespective of the location of the RFID registration unit and with sufficient inputs and outputs for all the wiring required for a door (access point).
- In situ wiring for all alarm contacts and door opening commands for the whole door.

The access control hub should not use any additional cables.

- Connection between the door manager and the registration unit by a single (coaxial) cable, which controls the opening mechanism of the locking element, visual feedback (red/green LED) and the acoustic signal transmitter of the antenna with coded (encrypted) signals.
- Modularity of the control unit and the antenna versions: Allow for different spheres of influence, resulting in different reading distances or areas depending on the identification medium.
- Off-line mode: Full functionality (master record, access profile, PIN code and biometric verification) when the connection to the access control hub is interrupted.
- All actions logged in off-line mode.
- Support of the function Support transport of authorisations on a medium (validation of media) function.
- Standard interface for the customised integration of special applications, such as generally available biometric registration units, elevator control systems, barcode scanners and wide-range solutions.
- Option to upgrade the firmware via the ethernet interface.
- Provide screw terminals that can be easily plugged into the door manager for wiring of the inputs and outputs.
- Option to add extra inputs and outputs to extension units without additional wiring or power supplies using plug and play.

Performance features: Provide the following:

- Identification segments: Unique number, Kaba Group header, Kaba advant ID, LEGIC access pool, LEGIC access, customer-specific definitions.
- Data segments: Kaba CardLink, LEGIC Biometric pool, Kaba Biometric.
- RFID standards support:
  . LEGIC prime with the industry standard LEGIC RF, LEGIC advant with the industry standards ISO/IEC 15693 and ISO/IEC 14443-1.
  . Other RFID standards with the industry standards ISO/IEC 15693 and ISO/IEC 14443-1.
- Extended off-line capability: Access decision based on company codes/badges and time-related authorisation including verification.

This feature provides:

- Saving of up to 10,000 badges, self-learning.
- The master record data must be automatically loaded to the door manager upon authorised booking (self-learning).
- Saving of up to 32 time zones.
- Logbook with up to 2000 entries.

- RS 485 interface:
  . Communication with access hub.
  . Electrically isolated, 2-wire.
  . Automatic baud rate detection (19200/9600 baud).
  . Terminating resistor for bus or star connection (jumper).
  . Addresses: 1 – 16 (rotary switch).
- HF LEGIC interface:
  . 2 antennas.
  . Coaxial cable, 50 ohms.
  . Interface to readers: Encrypted data transmission.
- RS 232 interface:

  . Connection for registration units (keypads and biometric solutions).
  . Integration options, wide-range solutions (e.g. Hyper X, Nedap AVI).
  . Output voltage 5 V d.c.
- Inputs:
  . Connections: Screw/plug terminals.
  . 4 line-monitored binary inputs with internal power supply and joint ground, for connection of potential-free contacts.
  . 1 internal input.
  . 1 tamper switch.
  . LED status display.
- Outputs:
  . Connections: Screw/plug terminals.
  . 3 relay outputs.
  . Changeover contact: maximum 2 A at 30 V a.c./d.c.
  . LED status display.
- General:
  . Mounting: DIN rail.
  . Dimensions 125 x 99 x 45 mm.
  . Operating temperature 0° to +50°C.
  . Protection type: IP40.
  . CE approval.
  . Standards: EN 55022, EN 55024, EN 60950-1.

Universal door manager

Selection: Kaba exos DMU2.

Options

Type: Kaba exos IC8.

Description: Extension module with 8 additional line-monitored inputs.

Type: Kaba exos OC8.

Description: Extension module with 8 additional outputs. 2 extension modules possible (total of 16 additional outputs).

Requirement: Provide a universal door manager that is able to connect readers from any manufacturer with its standardized Wiegand and Clock/Data interfaces and conforms to the following:

- Connection of up to 2 readers.
- Simple migration of existing systems.

It must be possible to continue using existing readers with media already in circulation.

- Installation in a tamper-proof place irrespective of the location of the reader with sufficient inputs and outputs for all the wiring required for a door (access point).
- Wiring for all alarm contacts and door opening commands in situ for the whole door.

The access control hub should not use any additional cables.

- Off-line mode: Full functionality (including master record, access profile, PIN code) when the connection to the access control hub is interrupted.
- All actions logged in off-line mode.
- Standard interface for the customised integration of special applications, such as generally available biometric registration units, elevator control systems, barcode scanners, wide-range solutions.
- Provide screw terminals that can be easily plugged into the door manager for wiring of the inputs and outputs.
- Option to add extra inputs and outputs to extension units without additional wiring or power supplies using plug and play.

Performance features: Provide the following:

- Connection of up to 2 readers with any media types.

- Extended off-line capability:
  . Access decision based on company codes/badges and time-related authorisation including verification.

This feature provides:

- Saving of up to 10,000 badges, self-learning.
- The master record data must be automatically loaded to the door manager upon authorised booking (self-learning).
- Saving of up to 32 time zones.
- Logbook with up to 2000 events.

- RS 232 interfaces:
  . 2 interfaces for the customised integration of special applications (readers, keypads).
  . Output voltage 5 V d.c.
  . Integration options, wide-range solutions (e.g. Hyper X, Nedap AVI).
- RS 485 interface:
  . Communication with access hub.
  . Electrically isolated, 2-wire.
  . Automatic baud rate detection (19200/9600 baud).
  . Terminating resistor for bus or star connection (jumper).
  . Addresses: 1 to 16 (rotary switch).
- Reader interfaces:
  . 2 interfaces.
  . Wiegand and Clock/Data.
  . Output voltage 5 V or 10 to 34 V (jumper).
  . 4 outputs each for control of visual and acoustic signal transmitters.
  . 1 tamper switch each.
- RS 232 interface:
  . 2 interfaces.
  . Connection for registration units (keypads and biometric solutions).
  . Integration options, wide-range solutions (e.g. Hyper X, Nedap AVI).
  . Output voltage 5 V d.c.
- Inputs:
  . Connections: Screw/plug terminals.
  . 4 line-monitored binary inputs with internal power supply and joint ground, for connection of potential-free contacts.
  . LED status display.
  . 1 tamper switch.
- Outputs:
  . Connections: Screw/plug terminals.
  . 3 relay outputs.
  . Changeover contact; maximum 2 A at 30 V a.c./d.c.
  . LED status display.
- General:
  . Mounting: DIN rail.
  . Dimensions 125 x 99 x 45 mm.
  . Operating temperature: 0° to +50°C.
  . Protection type: IP40.
  . CE approval.
  . Standards: EN 55022, EN 55024.

Access manager with integrated ethernet interface (IP)
Selection: Kaba exos iDML2.

Option 1

Type: Kaba exos IC8.

Description: Extension module with 8 additional line-monitored inputs.

Option 2

Type: Kaba exos OC8

Description: Extension module with 8 additional outputs. 2 extension modules possible (total of 16 additional outputs).

Requirement: Provide access manager which works with remote RFID registration units (antennas, PIN code, biometrics, on-line locks and cylinders) in combination with contactless RFID technology such as LEGIC and other industry standards, and includes the following functionalities:

- Door manager: Fully control, log and alarm one to two doors and make autonomous access decisions.
- Installation in a tamper-proof place irrespective of the location of the RFID registration unit with sufficient inputs and outputs for all the wiring required for a door (access point).
- Option to fully integrate 2 registration units or up to two doors.
- Wiring for all alarm contacts and door opening commands in situ for the whole door.

That is, the access control hub should not use any additional cables.

- Connection between the access manager and the registration unit by a single (coaxial) cable, which controls the opening mechanism of the locking element, visual feedback (red/green LED) and the acoustic signal transmitter of the antenna with coded (encrypted) signals.
- Direct connection to the access management system via the company's own network using an Ethernet interface.
- Encryption of data transmission to the higher level system with VPN/.
- Automatic software updates, including firmware updates, either by the higher level system or via a web interface.
- Modularity of the control unit and the antenna versions: Allow for different spheres of influence, resulting in different reading distances or areas, depending on the identification medium.
- Off-line mode: Full functionality (master record, access profile, PIN code and biometric verification) if the connection to the access control hub is interrupted.
- All actions logged in off-line mode.
- Two standard RS-232 interfaces for the customised integration of special applications, such as generally available biometric registration units, elevator control systems, barcode scanners, wide-range solutions.
- Support of the Support transport of authorisations on a medium function (validation and update of media).
- Provide screw terminals for that can be plugged into the door manager for wiring of the inputs and outputs.
- Option to add extra inputs and outputs to extension units without additional wiring or power supplies using plug-and-play.

Performance features: Provide the following:

- Connection of up to 2 remote antennas using a coded/encrypted signal.
- RFID technology: LEGIC advant with the industry standards ISO/IEC 15693, ISO/IEC 14443-1 and LEGIC RF.
- On-line mode: Access decision happens in higher level system (badge, time-based calculation).
- Off-line mode (operating mode in event of network interruption):
- Local access decision based on badge (badge, time-based authorisation, biometric verification).
- Automatic forwarding of events to the higher level system in network mode.
- Memory capacity for off-line mode:
  . 10,000 badges.
  . 100 time zones, 31 special days.
  . Logbook for 10,000 events.
  . 10 codes for access without badge (in combination with the PIN code keypad).

- Interfaces to the access management system:
  . Ethernet interface: (10/100 Mbit).
- HF LEGIC interfaces:
  . 2 antennas.
  . Coaxial cable, 50 ohms.
  . Encrypted data transmission.
- RS 232 interface:
  . 2 interfaces.
  . Connection for registration units (keypads and biometric solutions).
  . Integration options, wide-range solutions (e.g. Hyper X, Nedap AVI).
  . Output voltage 5 V d.c.
- Inputs:
  . Connections: Screw/plug terminals.
  . 4 line-monitored binary inputs with internal power supply and joint ground, for connection of potential-free contacts.
  . 2 internal inputs for door handle contact.
  . 1 tamper switch.
  . LED status display.
- Outputs:
  . Connections: Screw/plug terminals.
  . 3 relay outputs.
  . Changeover contact: maximum 2 A at 30 V a.c./d.c.
  . LED status display.
- Mounting: DIN rail.
- Dimensions: 125 x 99 x 45 mm.
- Ambient conditions:
  . Operating temperature 0° to +50°C.
  . Protection type: IP40.
- Power supply:
  . 10 to 34 V, maximum 4.5 W.
- Standards and approvals:
  . CE approval.
  . Standards: To EN 300330-2, EN 301489-1 and EN 301489-3.

Extension module with 8 outputs

Selection: Kaba exos OC8.

Requirement: As an optional addition to the door manager/access manager, provide up to two extension modules, each with 8 relay outputs, which include the following functionalities:

- Installation via a simple plug connection without additional wiring.

That is, the power supply to the extension module must be through the door manager/access manager.

- Outputs: LED status display.
- Option for the access management system and a local elevator control system to make free use of the outputs.
- Provide screw terminals that can be easily plugged into the extension module for wiring of the outputs.

Performance features: Provide the following:

- Mounting on DIN rail.
- Dimensions 70 x 99 x 45 mm.
- Power supply from door manager or access manager.
- Operating temperature 0° to +50°C.

- 10 to 34 V maximum 3.5 W.
- Protection type: IP40.
- CE approval.
- Standards: EN 55022, EN 55024.
- 8 relay outputs (total of 16 per door manager or access manager).
  . Connections: Screw / plug terminals.
  . Changeover contact; maximum 2 A at 30 V a.c./d.c.
  . LED status display.

Extension module with 8 line-monitored inputs

Selection: Kaba exos IC8.

Requirement: As an optional addition to the door manager/access manager, provide an extension module with 8 inputs, which meets the following requirements:

- Installation via a simple plug connection without additional wiring.

That is, the power supply to the extension module must be through the door manager/access manager

- Inputs: Line-monitored and fitted with an LED status display. Provide for separate deactivation.
- Option for the access management system to freely use the inputs.
- Provide screw terminals that can be easily plugged into the extension module for wiring of the inputs.

Performance features: Provide the following:

- Mounting on DIN rail.
- Dimensions 70 x 99 x 45 mm.
- Power supply from door manager or access manager.
- Operating temperature 0° to +50°C.
- Protection type: IP40.
- CE approval.
- Standards: EN 55022, EN 55024.
- 8 binary inputs:
  . Connections: Screw / plug terminals.
  . 5 V maximum 1 W.
  . Line-monitored (can be deactivated individually).
  . With internal power supply and joint ground for connection of potential-free contacts.
  . LED status display.

Flexible RFID antennas (registration units)

Selections: Provide the following:

- Kaba exos LA-PP (65 x 37 x 17 mm).
- Kaba exos LA-PB (70 x 70 x 10 mm).
- Kaba exos LA PV (130 x 130 x 11 mm).
- Kaba exos LA-KT (180 x 120 x 8 mm).
- Kaba exos LA-SK (200 x 450 x 22 mm).
- Kaba exos LA-SK (200 x 450 x 22 mm).
- Kaba exos LA-PC (32 x 48.5 mm).

Requirement: Provide antennas for a wide range of installation variants which combine with the door manager/access manager to form a fully integrated access reader with the following functionalities:

- Antenna: Suitable for both indoor and outdoor applications, depending on housing and installation.
- Ensure the functionality of a compact reader or door manager with a registration unit in metallic surroundings through the use of suitable antenna versions.
- Registration unit: Suitable for use both on-line, integrated into a system, and off-line with the door manager/access manager.
- Access reader: Supporting the Support transport of authorisations on a medium function (CardLink).

- Encryption of data transmission from the medium to the door manager.
- Connection between the door manager and the registration unit by a single (coaxial) cable, which controls the opening mechanism of the locking element, visual feedback (red/green LED) and the acoustic signal transmitter of the antenna with coded (encrypted) signals.
- Door opener relay and all relevant door contacts: Do not directly wire from the registration unit. Implement all door wiring from a tamper-proof place via the door manager.

Due to the fact that the antenna is installed remotely from the actual access reader, any antenna design is possible and adaptation to suit the spatial, architectural and security demands of a building or area must therefore be possible.

RFID antenna variants (registration units): Provide the following:

- Antennas for surface, flush or installation mounting:
  . Flush socket mounting (UP-I, various brands and designs), including in metallic surroundings.
  . Visible or invisible door panel installation.
  . Directly on door frame or door plate as documented.
  . Visible glass mounting.

For sliding doors.

- Column or wall mounting (installation in a plexiglass column).
- Antenna installation in an explosive protected housing.

For example, chemical/petroleum companies.

- At parking lot entrances.

Add additional requirements if required.

- Antennas for integration in existing light switch programs and intercom systems.
- Antennas for larger ranges.

Performance features: Provide the following:

- Connection type: Screw terminals for coaxial cable, 50 ohms: RG-178.
- Two-coloured LED (red/green) for indication of the operating mode and access decision.
- Buzzer for acoustic signalling of access decision.
- Reading distances: 10 mm to 300 mm, depending on the identification medium, installation conditions and antenna.
- Dimensions of antenna: 65 x 37 x ~17 mm to 200 x 450 x ~22 mm.
- Power supply from door manager.
- Operating temperature: -20° to +60°C.

Registration unit for surface mounting

Selection: Kaba exos LA-PG

Option 1

Selection: Kaba Card holder for Kaba exos LA-PG.

- For inserting the badge/key during the CardLink™ update.
- For inserting the badge/key for hold-open mode.

Option 2

Selection: Kava exos iDML2.

- For the operation of the Kaba exos LA-PG as an update reader.

Requirement: Provide a registration unit for surface mounting with LEGIC antenna which combines with the door manager to form a fully integrated access reader with the following functionalities:

- Suitable for mounting the registration unit on metal or glass surfaces.
- Suitable for both indoor and outdoor applications.
- Suitable for use both on-line, integrated into a system, and off-line with the door manager.
- Supporting the Transport of authorisations on a media function (validation of media).
- Supporting the Transport of authorisations on a media function (update of access authorisations).
- Encryption of data transmission from the medium to the door manager.

- Connection between the door manager and the registration unit by a single (coaxial) cable, which controls the opening mechanism of the locking element, visual feedback (red/green LED) and the acoustic signal transmitter of the antenna with coded (encrypted) signals.
- Door opener relay and all relevant door contacts: Do not directly wire from the registration unit. Implement all door wiring from a tamper-proof place via the door manager.

Performance features: Provide for the following:

- Mounting: Adhesive or screw mounting.
- Connection type: Screw terminals for coaxial cable, 50 ohms: RG-178.
- Two-coloured LED (red/green) for indication of the operating mode and access decision.
- Buzzer for acoustic signalling of access decision.
- Reading distance: Up to 100 mm.
- Dimensions of housing: 87.5 x 87.5 x 18 mm.
- Power supply from door manager/access manager.
- Operating temperature -20° to +60°C.
- Protection type: IP54.
- CE approval.
- Standards: EN 300330, ETS 300683.

Small registration unit for surface mounting and metallic surroundings

Selection: Kaba.

Type: Kaba exos LA-PC.

Requirement: Provide a registration unit for surface mounting with integrated LEGIC antenna which combines with the door manager/access manager to form a fully integrated access reader with the following functionalities:

- Suitable for mounting the registration unit directly on the door frame or a door plate.
- Suitable for both indoor and outdoor applications.
- Suitable for use both on-line, integrated into a system, and off-line with the door manager/access manager.
- Reader: Supporting the Support transport of authorisations on a medium (CardLink) function.
- Encryption of data transmission from the medium to the door manager.
- Connection between the door manager and the registration unit by a single (coaxial) cable, which controls visual feedback (red/green LED) and the acoustic signal transmitter of the antenna with coded (encrypted) signals.

Performance features: Provide the following:

- Mounting: Adhesive or screw mounting.
- Connection type: Screw terminals for coaxial cable, 50 ohms: RG-178.
- Two-coloured LED ring (red/green) for indication of the operating mode and access decision.
- Buzzer for acoustic signalling of access decision.
- distance up to approx. 50 mm.
- Dimensions of housing: Rectangular/oval, 48.5 x 32 x 18.5 mm).
- Power supply from door manager/access manager.
- Operating temperature -20° to +60°C.
- Protection type: IP55.
- CE approval.
- Standards: EN 300330, ETS 300683.

PIN code keypad with housing for surface mounting

Selection: Kaba exos LT-PN.

Requirement: Provide a registration unit for surface mounting with integrated LEGIC antenna and keypad which combines with the door manager to form a fully integrated access reader with the following functionalities:

- Option to define the PIN code verification requirements for verification of the user (medium) depending on time.

For example, access must be possible during the day with normal badge identification alone but only with badge and PIN code at night.

- Registration unit with keypad suitable for mounting on metal or glass surfaces.
- Suitable for both indoor and outdoor applications.
- Suitable for use both on-line, integrated into a system, and off-line with the door manager.
- Reader support of the Support transport of authorisations on a medium (CardLink) function.
- Encryption of data transmission from the medium to the door manager.
- Door opener relay and all relevant door contacts: Do not directly wire from the registration unit. Implement all door wiring from a tamper-proof place via the door manager.
- Option to input a door opening code for access without a badge.

Performance features: Provide the following:

- Mounting: Adhesive or screw mounting.
- Connection type: Screw terminals for coaxial cable, 50 ohms: RG-178.
- Two-coloured LED (red/green) for indication of the operating mode and access decision.
- LED (yellow) for PIN code request.
- LED (red/yellow) for special function.
- Buzzer for acoustic signalling of access decision.
- Reading distance: Up to approx. 100 mm.
- Dimensions of housing: 87.5 x 87.5 x18 mm.
- Power supply from door manager / access manager.
- Operating temperature -20° to +55°C.
- Protection type: IP55.
- CE approval.
- Standards: EN 300330, ETS 300683.

Registration unit for biometric verification with housing for surface mounting

Selection: Kaba exos Biover II.

Requirement: Provide a registration unit for surface mounting with integrated LEGIC antenna and biometric verification which combines with the door manager/access manager to form a fully integrated biometric access reader with the following functionalities:

- Biometric verification of fingerprint data in addition to normal identification with a badge.
- With respect to data protection, no database of biometric data may be kept, i.e. fingerprint data (templates) are stored directly on a LEGIC medium.
- Option to store the templates of two different fingers on the LEGIC medium.
- Option to define whether or not biometric verification is required depending on time.

For example, access must be possible during the day with normal badge identification alone but only with badge and biometric verification at night.

- Option to store biometric data at one central location or at several decentralised locations in the system network.
- Registration unit with keypad suitable for mounting on metal or glass surfaces.
- Suitable for both indoor and outdoor applications.
- Provide small biometric registration unit for use in interlocking doors or isolating systems with maximum dimensions of 88.5 x 88.5 x 35.2 mm.
- Suitable for use both on-line, integrated into a system, and off-line with the door manager.
- Reader support of the Support transport of authorisations on a medium (CardLink) function.
- Encryption of data transmission from the medium to the door manager.
- Provide an integrated tamper switch blocking the functionality of the biometric unit when the housing is opened.
- Installation-compatible with the registration unit with PIN code keypad, to allow PIN code verification installed today to be quickly and easily upgraded for higher security requirements with biometric verification.

Performance features: Provide the following:

- Biometric sensor: High-resolution biometric thermal line sensor.
- Medium for biometric data: LEGIC prime Supertag, LEGIC 15693.
- Maximum memory required for biometric templates on the LEGIC medium: 340 bytes.
- Mounting: Adhesive or screw mounting.
- Connection type: Screw terminals for coaxial cable, 50 ohms: RG-178.
- LED (red/green/orange) for indication of the operating mode and access decision.
- LED (orange/red) for biometric request/decision.
- Buzzer for acoustic signalling of access decision.
- Reading distance: Up to approx. 100 mm.
- Dimensions of housing: 88.5 x 88.5 x 35.2 mm.
- Power supply from door manager.
- Operating temperature -20° to +50°C.
- Protection type: IP54.
- CE approval.
- Standards: EN 300330, ETS 300683.

Compact registration unit/Door manager for indoor areas

Selection: Kaba exos cDML.

Option

Selection: Kaba exos 9300.

Type: Spacer frame for Kaba exos cDML.

- Spacer frame for surface cable routing.

Requirement: Provide a compact door manager (access reader) which works with an integrated registration unit in combination with contactless RFID technologies such as LEGIC and other industry standards and includes the following functionalities:

- Wiring for the necessary alarm contacts and door opening commands in situ for the whole door.

That is, the access control hub should not use any additional cables.

- Quick and straightforward wiring possible using a baseplate with edge connector without having to mount the reader electronics.
- Feeding in cable using surface mounting or flush mounting.
- Support of the Support transport of authorisations on a media (validation of media) function.
- Automatic loading of the master record data to the door manager upon authorised booking (self-learning).
- Off-line mode: Full functionality (master record and access profile check) if the connection to the access control hub is interrupted.
- All actions logged in off-line mode.

Performance features: Provide the following:

- Support of RFID standards:
  - . LEGIC prime with the industry standard LEGIC RF, LEGIC advant with the industry standards ISO/IEC 15693 and ISO/IEC 14443-1.
  - . Other RFID standards with the industry standards ISO/IEC 15693 and ISO/IEC 14443-1 memory capacity: up to 10,000 badges (depending on media), self-learning.
- On-line mode: Access decision occur in higher level system (badge, time-based calculation).
- Off-line mode (interruption to communication):
  - . Local access decision (badge, time-based authorisation).
  - . 32 time zones.
  - . Logbook for 2 000 events.
- RS 485 interface:
  - . Communication with access hub.
  - . Electrically isolated, 2-wire.

  . Automatic baud rate detection (19200/9600 baud).
  . Terminating resistor for bus or star connection (DIP switch).
  . Addresses: 1-16 (DIP switch).
- HF LEGIC interface:
  . Integrated registration unit.
  . Encrypted data transmission.
- Inputs:
  . 2 binary inputs for door opener key/frame contact/door handle contact.
  . Line-monitored, 8 can be deactivated).
  . LED status display.
- Outputs:
  . 1 for door opener activation.
  . 1 tamper switch for external tamper monitoring (additional wiring to hub required).
- Connections: Screw terminals, maximum 5A.
- Mounting: Quick connection.
- Dimensions:
  . For concealed cables: 87.5 x 87.5 x 18 mm.
  . For surface cables: 87.5 x 87.5 x 25 mm.
- Signalling:
  . Two-coloured LED (red/green) for indication of the operating mode and access decision.
  . Buzzer for acoustic signalling of access decision.
- Power supply:
  . AC 12 27 V 50/60Hz, 12 to 32 V.
  . Power consumption: maximum 2 VA.
- Ambient conditions:
  . Operating temperature: 0° to +50°C.
  . Protection type: IP40 (indoors).
- CE approval.

PC desktop reader with USB interface

Selection: Kaba B-Net 9107 desktop reader.

Requirement: Provide a PC desktop reader connected to a PC by a USB interface and including the following functionalities:

- Read/write badge data via a connection with the access management system permitting search for persons in the staff master data.
- Together with a personal badge, secure PC access without requirement for separate login.
- In conjunction with the Badge management option, location of badge data.
- In conjunction with the Transport of authorisations on a medium option, modification and validation of access authorisations for stand-alone components with a Web Client, over the company's own intranet.
- In conjunction with the Transport of authorisations on a medium option, modification and validation of access authorisations for stand-alone components with an interactive workstation, over the company's own intranet.
- In conjunction with the Transport of authorisations on a medium option, option to program the relevant segment on the medium with an interactive workstation, depending on operator rights.
- In conjunction with the Visitor management option, issue of visitor badges.
- In conjunction with the Registration unit for biometric verification option, biometric templates written to the badge with the PC desktop reader.
- In conjunction with the Programming of LEGIC badge segments option, biometric templates written to the badge with the PC desktop reader.
- A communication driver for integration in any given application.

Performance features: Provide the following:

- RFID technology: LEGIC advant with the industry standards ISO/IEC 15693, ISO/IEC 14443-1 and LEGIC RF.
- Interface: USB Version 2.0.
- Power supply via USB interface.
- Dimensions of housing: 85 x 54 x 13 mm.
- Cable length: 1.6 m.
- Operating temperature 0° to +40°C.
- Protection type: IP40.
- CE approval.

Mechatronic door furniture (stand-alone access control integration)

Selection: Kaba c-lever.

The Kaba elolegic c-lever door furniture excels in high user friendliness, elegant design and compact dimensions. The electronics, integrated in the inside door shield recognise keys, badges or other media without contact.

Ideal for operation access control areas, where audit logs are not required instantly, such as meeting rooms, offices and areas where cabling is not possible.

Advantages:

- Easy upgrade of existing mechanical door locks to a mechatronic stand alone access system.
- Used in conjunction with standard MS Mortice Lock or other equivalent Australian style Mortice Locks.
- Lock and cylinder independent.
- Increased operational safety with maximum flexibility.
- Simple and fast installation.
- No wiring required.
- Easy to program and operate.
- Simple maintenance.
- Transaction memory for the last 1 000 door movements.
- Can be used on panic doors.
- Fire-rated.
- Modes of operation include stand-alone or Integrated in the on-line world of Kaba exos with CardLink™.

Control of cabinets (stand-alone access control integration)

Selection: Kaba Locker Lock.

Designed for various cabinet and wardrobe applications in hospitals, care homes, universities, schools, transportation or in business areas. The battery-driven locker lock can be administered centrally, or by stand-alone methods. This way, a flexible programming and allocation of access rights can be realised.

Existing media like keys, badges or key fobs are applicable.

A low battery status is signalised on time so that below a certain level, the door cannot be closed anymore. A special battery replacement tool prevents vandalism and reflects the smart concept.

The FreeChoice operating mode allows the user a free choice of any open cabinets. After closing the cabinet, the media is automatically programmed – an ideal wardrobe function within a shared changing room.

The solid and splashproof design enables a multitude of applications.

2.7 INTRUDER ALARM

Volumetric detection devices

General: Provide volumetric detectors as documented.

Requirement: Provide detection within the space occupied by the detector. Provide additional detectors to achieve coverage as necessary.

Movement detectors are defined in AS 2201.3 at clause 1.4.9.

Sufficient detectors should be installed to provide full coverage of the designated areas. They should be mounted to avoid detection of movement outside the designated areas, which are best indicated on the drawings.

PIR detectors: Mirror optic type with ≥ 7 curtains.

Installation: To AS/NZS 2201.1.

Door contacts

Requirement: Provide concealed magnetic reed switches which operate when:

This includes magnetic reed switches in door frames, and heavy duty reed switches for vehicular doors.

- A personnel door is opened > 20 mm at the lock/latch edge.
- The fixed leaf of a double door is opened > 20 mm at the lock/latch edge.
- A vehicular door is opened > 100 mm.

Door lock sensors: Provide micro switches or magnetic contacts in lock keepers or door locks which incorporate a bolt movement sensing device.

Specify the type required, such as micro switches in the lock keeper or reed switches.

Function: To detect bolt movements > 10 mm.

2.8 DURESS ALARM

General

Requirement: Provide duress alarm switches as documented.

Desk or furniture mounting: Provide plug socket connections for duress alarm switches fixed to items of furniture. Conceal wiring and secure to avoid accidental disconnection.

Wall mounting: Recessed at 900 mm above finished floor level.

Disconnection alarm: Connect so that removal of plugs from sockets will automatically register as a duress alarm.

2.9 VIDEO MONITORING

CCTV system

General: Provide a closed circuit television system monitoring and recording the areas/spaces as documented.

Specify or schedule the total system video and audio performance to suit the security risk and monitoring procedures as determined in the site security manual.

CCTV cameras

Cameras should be suitable for their operating environment e.g. protective enclosures if likely to be damaged.

Note whether or not the cameras require a local power supply. If so, arrange for mains power to be provided.

Make sure that the sensitivity of the camera allows full coverage of the nominated areas throughout the full range of anticipated ambient lighting conditions. Arrange for additional lighting if required.

Show the position of remote control cameras and the controlled functions such as pan, tilt and zoom as well as the location of remote control point.

Requirement: Provide cameras selected to provide coverage of designated areas and to enable persons within the field of view to be readily distinguishable on monitors under all ambient night and day lighting conditions.

Where fixed next to or above doorways, persons standing at the door should be readily identifiable from the monitor. Where used to cover large areas, the coverage should be such that a person moving within the area can be easily seen, not necessarily identified, from the monitor. In most cases the nomination of particular focal length and aperture lenses should be left to the camera installer so that site conditions and exact mounting location can be taken into account, therefore when preparing the documents, only nominate the area to be covered.

Specify remote controlled zoom lenses with a focal range to meet the project specific requirements, where necessary.

Motorised cameras: Provide camera drives which provide remote control of camera rotation and tilt, and of lens focal length.

Delete if not required.

External cameras: Provide corrosion-resistant weatherproof housings for externally located cameras, which allow cameras to perform to manufacturer's specification.

Fixing: Provide mounting brackets and hardware which rigidly fix cameras, monitors and accessories to buildings or structures.

CCTV monitors

General: Provide LCD colour monitors compatible with the security system, and provide fixing brackets and hardware for wall-mounted and ceiling-mounted monitors.

The monitor parameters must match the cameras provided.

CCTV recording system

CCTV recorders may be available in several different forms. The simplest form is the video cassette recorder. To avoid overwriting sensitive data in this system, the user must remove the VCR tapes and store them. Typically a 7 or 14 day cycle is used for the re-use of VCR tapes.

Digital CCTV recording systems hold the information on a large capacity magnetic storage medium such as a hard disk, and the data can be interrogated in detail. It is common practice to provide a copy of sensitive data as a backup off site. Specify the system to be used or delete if not required.

General: Provide CCTV recording hardware and software systems which store data from each camera in an industry standard compressed digital format.

Functionality: Provide the following:

- Index according to events.
- Fast search.
- Frame-by-frame search.
- Frame printing.
- Zoom and pan within a recorded frame.
- Back up daily to off-site storage.

Minimum data storage: 30 days.

CCTV video switching system

General: Provide switching software which enables each camera to be directed to a specific monitor or for cameras to be scanned sequentially at predetermined intervals to a specific monitor and which, on receipt of an alarm signal, interrupts the scanning sequence and switches to the relevant security zones.

Delete if not required.

3 EXECUTION

3.1 GENERAL

Mains supplies

See AS 2201 clause 3.11. Ascertain emergency power requirements. Specify the capacity and duration for UPS or battery back up, and, for package contracting, clearly define the area of responsibility for the supply and installation of the system i.e. the security contractor, electrical contractor or builder.

Nominal operating voltage should be 12 V.

Show the location of required power outlets for panels and door controllers.

Permanent power supply: Provide permanent power supply to the following:

- Intruder alarm panels and access control panels including sub panels.
- Electric door strike local panels or control equipment.
- Intercom stations.
- CCTV monitors and cameras.

Marking: Label the switchboard circuit breaker from which power for the security systems is obtained: *SECURITY SYSTEM - Do not switch off*.

CCTV cameras

Positioning and adjustment: Position and aim cameras to provide optimum coverage and to minimise the effect of shadows or direct light sources.

Interconnection to other services

General: Provide functions and equipment to allow the interconnection to other systems. Provide and connect wiring to the designated services.

Lifts: Arrange for installation and connection of lift readers and associated equipment.

Describe the method of interconnection to other services such as lifts, air conditioning, lighting, and the location of readers. Specify services to be connected.

For lift control, designate the lifts that require readers – readers are usually supplied by the security contractor but installed and connected by the lift company responsible for the lift maintenance. Allow for the work associated with this, in package contracting.

For air conditioning control, where after hours air conditioning is activated by the access control system, clearly define the area of responsibility for interconnection to the mechanical services. Allow for the associated work.

For the intercommunication system, indicate the location and capacity of master and slave intercom stations, and coordinate with the access control or closed circuit television system. For external locations, requirements for weather proofing and tamper resistance should be taken into account.

Connection to telecommunications cabling may bring the installation under ACA control. Refer to AS/CA S009.

Completion tests

Provide details of specific testing requirements. See AS 2201.3 Appendices A to L for detection devices.

General: Carry out tests, including out-of-hours tests, to demonstrate the security system's performance. Include the following:

- Test components for correct function and operation.
- Demonstrate that devices perform on site, to at least the level stated in the manufacturer's performance specification for that device.
- Test the operation of alarm sectors and panel functions, including open and short circuit tests.
- Demonstrate that the system functions under mains fail condition.
- Demonstrate operation of the battery and charger including a full discharge/recharge over the designated time.

Maintenance:

Detail activities to be carried out during the maintenance period to suit the project. Do not specify testing by the building owner.

Standard: To AS/NZS 2201.1.

See AS/NZS 2201.1 Section 5, which is geared to maintenance agreements and describes some building owner obligations.

Breakdown call outs: Attend on site within 24 hours of notification. Rectify faults, and replace faulty materials and equipment.

Frequency of routine visits: ≤ 3 monthly.

Maintenance period performance monitoring:

- Monitor: Access control system.
- Investigate: Causes of alarms.
- Alarm report: < 2 days after alarm.

False alarms:

- Notification of false alarms: On the first working day after a false alarm, submit notification of the circumstances surrounding the false alarm and action necessary to prevent similar occurrences.
- Alterations due to false alarms: Carry out alterations necessary to eliminate false alarms due to the following:
- Technical faults, selection, siting or aiming of devices.
- Environmental conditions evident at the time of installation.

4 SELECTIONS

Schedules are a way of documenting a selection of proprietary or generic products or systems by their properties. Provide their locations here and/or on the drawings. When showing items in both places, identify them with a common code or tag to assist coordination. **Schedules** are well suited to multiple variants of the same item. If there is only a single instance of different items, a simple list may be sufficient. Make sure there is an entry for every item documented.

Duplicate and customise these **Schedules**, adding and deleting rows and columns, as required, e.g. delete rows if the selection is by the contractor or a proprietary product is selected. A proprietary product is usually selected on the basis of the properties it embodies, so there is generally no need to spell them out in a schedule – an exception being where they relate to options to, or variations from, a standard product.

4.1 SYSTEM DESCRIPTION

System description schedule

Security classification	
System communications	

Security classification: Nominate the security classification in conformance with AS/NZS 2201.1 Table A1.

Security communications: Nominate the type of communications system to suit the project specific requirements, e.g. proprietary, hard-wired, IT LAN, Wireless, IP based etc.

4.2 SECURITY MONITORING SYSTEMS

Security monitoring systems schedule

Monitoring system	
Communication method	
Base station location/identification	
Alarm response time	
Alarm system	
External audible and visual alarms	
Central monitoring facility	
Location	
Computer specification	
Event logging printer	
Uninterruptible power supply capacity (hours)	
Backup medium and capacity	
Interconnected systems	

Communication method: Ascertain method of connection to remote base station, if required. Allow for the work associated with connection, such as charges for line rental and connection.

Alarm response time: Specify alarm response time category to AS 2201.2.

Central monitoring facility: Delete if monitoring is not required. For local monitoring, indicate the location of the monitoring system or security control room, and whether additional mimic panels are required.

Interconnected systems: Describe the systems interconnected to the access control system. In particular consider:

- Lift car controls, floors covered, location of readers, hours of operation.
- After hours air conditioning control, location of readers, hours of operation. It may be prudent to handle this through a building management system rather than permitting mechanical personnel to access the access control system.

For lift control, designate the lifts that require readers - readers are usually supplied by the security contractor but installed and connected by the lift company responsible for the lift maintenance.

For air conditioning control, where after hours air conditioning is activated by the access control system, clearly define the area of responsibility for interconnection to the mechanical services.

Power requirements: If the power for controller panels is not to be provided as a part of this worksection, then the power requirements should be scheduled for the contractor.

4.3 ACCESS CONTROL SYSTEMS

Access control system schedule

System type	
Activation method	
De-activation method	
Other entry method	
Equipment mounting and enclosure	
Number of users to have unique codes	
Number of programmable time zones for automatic access	
Number of programmable access zones for	

automatic access	
Entry points	
Door control devices	
Internal access zones	
Delayed access zones	
Intercom function	
Remote operation function	
Vehicle control points	
Spare capacity	
Number of users	
Alarm zones	
Power supply	
Communication system	

Activation method: Specify the particular method of obtaining entry for each door, typically:

- Magnetic readers, proximity, card or key. For cards or keys, specify the type of card or key to be supplied and the quantity, including the quantity of pre-programmed cards or keys to be supplied for future issue.
- Key pads, with PIN programming.
- Intercom and remote operation.
- Remote, generally combined with an intercom.

Indicate whether local readers or key pads are to operate as stand alone units in the event of failure in the main processor system.

Entry points: Specify the number of controlled entry/exit doors, as well as the number of monitored (but not necessarily controlled) doors, to be connected to the system. Also consider entry/exit delay. Include spare capacity, and event logging system. Consider local or remote programming of system to accept/reject entry attempts.

Door control devices: Usually this should be cross referenced to the architectural door schedule. The schedule should list the individual doors together with the method of releasing or securing them. Take into account fire safety regulations, including fail safe operation, for means of egress from controlled doors, and magnetic holders for glass doors etc. State whether or not strikes are to incorporate microswitches. Distinguish double leaf doors from single leaf doors (solid frame) and state whether the wiring to double leaf doors is to be concealed or not.

Internal access zones: Specify the number of sectors required, generally separating internal zones from perimeter zones.

Delayed access zones: Identify the areas requiring delayed entry sectors - these should be kept to a minimum – and indicate the time range required. This should just be sufficient for a person familiar with the system to activate it.

Intercom function: Specify the type and location of intercom points.

Vehicle control points: Specify the particular method of obtaining entry, typically to match internal door activation. Describe the method of vehicle entry/exit to be provided i.e. boom gates, roller shutters, gates.

- Exit: Push-button, or to match the entry system.
- Interlock: To prevent the door from closing before the vehicle has left the exit point.
- Push-buttons and readers: Ensure that these are located within easy reach of the driver's side window.

Spare capacity: Indicate the spare capacity (number of sectors or zones) required. Some systems will require space for plug-in modules, for others they can be expanded by programming.

Power supply: Ascertain emergency power requirements. Specify the capacity and duration for UPS or battery backup, and, for package contracting, clearly define the area of responsibility for the supply and installation of the system i.e. the security contractor, electrical contractor or builder. Nominal operating voltage should be 12 V.

4.4 INTRUDER ALARM SYSTEMS

Intruder alarm system schedule

Security risk classification to AS/NZS 2201.1	
System type	

Intruder alarm zones	
Detector types	
Activation device type	
Activation method	
De-activation method	
Number of activation devices to be provided including programming	
Interconnection requirements for other systems	Access control system Local monitoring system Remote monitoring system
Spare capacity	25% of alarm zones
Communication system	

Detector types: Specify the type of detector to be provided for each protected location.

- Internal space detection: Passive infra-red, ultrasonic microwave, pressure mats, etc., taking into account the relative advantages and disadvantages of each. See AS 2201.3, which describers many types as well as general requirements. Use the same terminology, including types and categories, as the standard.
- Perimeter: Reed switches, micro switches, photo electric beams.

Activation method: Specify the particular method of activating each zone, typically:

- Magnetic readers, proximity, card or key. For cards or keys, specify the type of card or key to be supplied and the quantity, including the quantity of pre-programmed cards or keys to be supplied for future issue.
- Key pads, with PIN programming.
- Intercom and remote operation.
- Remote, generally combined with an intercom.

Indicate whether local readers or key pads are to operate as stand alone units in the event of failure in the main processor system.

4.5 DURESS ALARMS

Duress alarm schedule

System type	
Alarm button type – wall mounted	
Alarm button type – desk/furniture mounted	
Alarm response	

4.6 CCTV MONITORING SYSTEM

CCTV system schedule

System type	
Communications system	

Camera schedule

Camera(s) fixed – location and type	
Camera(s) pan/tilt/zoom – location and type	
Camera(s) dome – location and type	
Lens types and mounts	

Scanning system	
Resolution	
Signal to noise ratio	
Minimum illumination for useable video	

CCTV cameras: Schedule the type and features of the CCTV cameras required for the project. Fixed lens cameras may be useful for corridors and doors. Pan tilt zoom cameras may be used to cover multiple locations by pre-programming preset response positions according to predetermined events. It is common practice for the CCTV lens to be selected by the contractor during installation to suit the application. CCTV lens characteristics such as field of view and focal length are not readily specified and depend on the final CCTV camera location. Where a particular lens is required, this should be included in the schedules.

Monitor schedule

Location and type	
Resolution	
Colour system	
Video input	

Recording system schedule

Location and type	
Recording rate	
Recording modes	
Resolution	
Colour system	
Video/audio input	
Video/audio output	

Schedule the type, number and location of the CCTV recording system. Schedule the backup site location, if any, and the interconnection method.

REFERENCED DOCUMENTS

The following documents are incorporated into this worksection by reference:

EN 300330	2010	Electromagnetic compatibility and radio spectrum matters (Erm) - Short range devices (Srd) - Radio equipment in the frequency range 9 Khz to 25 Mhz and inductive loop systems in the frequency range 9 Khz to 30 Mhz
EN 301489		Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility (EMC) standard for radio equipment and services
EN 301489-1	2010	Common technical requirements
EN 301489-3	2001	Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz
EN 55022	2010	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
EN 55024	2010	Information technology equipment - Immunity characteristics - Limits and methods of measurement
ETS 300683	1997	Radio equipment and systems (RES) - Electromagnetic compatibility (EMC) standard for short range devices (SRD) operating on frequencies between 9 Khz and 25 Ghz
ISO/IEC 14443-1	2008	Physical characteristics
ISO/IEC 15693		Identification cards - Contactless integrated circuit(s) cards - Vicinity cards
AS/NZS 2201		Intruder alarm systems
AS/NZS 2201.1	2007	Client's premises - Design, installation, commissioning and maintenance
AS 2201.3	1991	Detection devices for internal use
AS 2201.4	1990	Wire-free systems installed in client's premises
AS/NZS 2201.5	2008	Alarm transmission systems
AS 4262		Telecommunication overvoltages
AS 4262.1	1995	Protection of persons
AS 4262.2	1999	Protection of equipment
AS 4806		Closed circuit television (CCTV)

AS 4806.2	2006	Application guidelines
AS 4806.4	2008	Remote video
EN 300330-2	2006	Harmonized En Covering The Essential Requirements of Article 3.2 Of The R&tte Directive
EN 60950	2000	Safety of information technology equipment
EN 60950-1	2006	General Requirements
ISO/IEC 14443		Identification cards - Contactless integrated circuit cards - Proximity cards
The following documents are mentioned only in the *Guidance* text:		
AS/CA S009	2013	Installation requirements for customer cabling (Wiring Rules)
AS 2201	various	Intruder alarm systems
AS 2201.2	2004	Monitoring centres
NATSPEC GEN 006	2007	Product specifying and substitution
NATSPEC TECHreport	2013	Specifying ESD
NATSPEC TECHreport	2013	Selection and design of building IT systems